We only use cookies that are necessary for this site to function to provide you with the best experience. The controller of this site may choose to place supplementary cookies to support additional functionality such as support analytics, and has an obligation to disclose these cookies. Learn more in our Cookie Statement.

Subscribe to updates from Cybersecu
Infrastructure Security Agency

Email Address e.g. name

Subscribe

Share Bulletin

Vulnerability Summary for the Week of November 1, 2021

Cybersecurity and Infrastructure Security Agency sent this bulletin at 11/08/2021 01:21 PM EST

You are subscribed to National Cyber Awareness System Bulletins for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

Vulnerability Summary for the Week of November 1, 2021

11/08/2021 09:21 AM EST

Original release date: November 8, 2021

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aaptjs_project -- aaptjs	An issue was discovered in the crunch function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	2021-10-31	7.5	CVE-2020-36380 MISC
aaptjs_project -- aaptjs	An issue was discovered in the remove function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	2021-10-31	7.5	CVE-2020-36379 MISC
aaptjs_project -- aaptjs	An issue was discovered in the list function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	2021-10-31	7.5	CVE-2020-36376 MISC
aaptjs_project -- aaptjs	An issue was discovered in the dump function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	2021-10-31	7.5	CVE-2020-36377 MISC
aaptjs_project -- aaptjs	An issue was discovered in the packageCmd function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	2021-10-31	7.5	CVE-2020-36378 MISC
aaptjs_project -- aaptjs	An issue was discovered in the singleCrunch function in shenzhim aaptjs 1.3.1, allows attackers to execute arbitrary code via the filePath parameters.	2021-10-31	7.5	CVE-2020-36381 MISC
aaptjs_project -- aaptjs	An issue was discovered in the add function in Shenzhim AAPTJS 1.3.1 which allows attackers to execute arbitrary code via the filePath parameter.	2021-10-31	7.5	CVE-2020-26707 MISC
apache -- traffic_server	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability in the stats-over-http plugin of Apache Traffic Server allows an attacker to overwrite memory. This issue affects Apache Traffic Server 9.1.0.	2021-11-03	7.5	CVE-2021-43082 MISC
beckhoff -- tf6100_firmware	TwinCAT OPC UA Server in TF6100 and TS6100 in product versions before 4.3.48.0 or with TcOpcUaServer versions below 3.2.0.194 are prone to a relative path traversal that allow administrators to create or delete any files on the system.	2021-11-04	8.5	CVE-2021-34594 CONFIRM
church_management_system_project -- church_management_system	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Church Management System 1.0 via the image upload field.	2021-10-29	7.5	CVE-2021-41643 MISC
cisco -- anyconnect_secure_mobility_client	A vulnerability in the Network Access Manager (NAM) module of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to escalate privileges on an affected device. This vulnerability is due to incorrect privilege assignment to scripts executed before user logon. An attacker could exploit this vulnerability by configuring a script to be executed before logon. A successful exploit could allow the attacker to execute arbitrary code with SYSTEM privileges.	2021-11-04	7.2	CVE-2021-40124 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- catalyst_pon_switch_cgp-ont-1p_firmware	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory.	2021-11-04	7.5	CVE-2021-34795 CISCO
cisco -- catalyst_pon_switch_cgp-ont-1p_firmware	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory.	2021-11-04	7.5	CVE-2021-40113 CISCO
cisco -- ios_xr	A vulnerability in the web-based management interface of certain Cisco Small Business RV Series Routers could allow an authenticated, remote attacker with administrative privileges to inject arbitrary commands into the underlying operating system and execute them using root-level privileges. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending malicious input to a specific field in the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system as a user with root-level privileges.	2021-11-04	9	CVE-2021-40120 CISCO
customer_relationship_management_system_project -- customer_relationship_management_system	An SQL Injection vulnerability exists in Sourcecodester Customer Relationship Management System (CRM) 1.0 via the username parameter in customer/login.php.	2021-11-03	10	CVE-2021-43130 MISC
dlink -- dir-823g_firmware	An issue in the component /cgi-bin/upload_firmware.cgi of D-Link DIR-823G REVA1 1.02B05 allows attackers to cause a denial of service (DoS) via unspecified vectors.	2021-11-04	8.5	CVE-2020-25366 MISC MISC MISC
dlink -- dir-823g_firmware	A command injection vulnerability was discovered in the HNAP1 protocol in D-Link DIR-823G devices with firmware V1.0.2B05. An attacker is able to execute arbitrary web scripts via shell metacharacters in the Captcha field to Login.	2021-11-04	7.5	CVE-2020-25367 MISC MISC MISC
dotty_project -- dotty	This affects the package dotty before 0.1.2. A type confusion vulnerability can lead to a bypass of CVE-2021-25912 when the user-provided keys used in the path parameter are arrays.	2021-11-03	7.5	CVE-2021-23624 MISC MISC
doyocms_project -- doyocms	Arbitrary file upload vulnerability sysupload.php in millken doyocms 2.3 allows attackers to execute arbitrary code.	2021-11-01	7.5	CVE-2021-26740 MISC
doyocms_project -- doyocms	SQL Injection vulnerability in pay.php in millken doyocms 2.3, allows attackers to execute arbitrary code, via the attribute parameter.	2021-11-01	7.5	CVE-2021-26739 MISC
duraspace -- dspace	DSpace is an open source turnkey repository application. In version 7.0, any community or collection administrator can escalate their permission up to become system administrator. This vulnerability only exists in 7.0 and does not impact 6.x or below. This issue is patched in version 7.1. As a workaround, users of 7.0 may temporarily disable the ability for community or collection administrators to manage permissions or workflows settings.	2021-10-29	9	CVE-2021-41189 MISC MISC CONFIRM MISC
e-negosyo_system_project -- e-negosyo_system	An SQL Injection vulnerability exists in Sourcecodester E-Negosyo System 1.0 via the user_email parameter in /admin/login.php.	2021-10-29	7.5	CVE-2021-41674 MISC MISC MISC
eclipse -- paho_mqtt_c\/c_client	In versions prior to 1.1 of the Eclipse Paho MQTT C Client, the client does not check rem_len size in readpacket.	2021-11-03	7.5	CVE-2021-41036 CONFIRM
ed01-cms_project -- ed01-cms	ED01-CMS v1.0 was discovered to contain a SQL injection in the component cposts.php via the cid parameter.	2021-11-03	7.5	CVE-2020-18262 MISC
ed01-cms_project -- ed01-cms	An arbitrary file upload vulnerability in the image upload function of ED01-CMS v1.0 allows attackers to execute arbitrary commands.	2021-11-03	7.5	CVE-2020-18261 MISC
ericsson -- network_location_mps_gmpc21	In Ericsson Network Location MPS GMPC21, it is possible to inject commands via file_name in the export functionality.	2021-11-03	7.5	CVE-2021-43339 MISC MISC
eyoucms -- eyoucms	SQL Injection vulnerability in eyoucms cms v1.4.7, allows attackers to execute arbitrary code and disclose sensitive information, via the tid parameter to index.php.	2021-11-03	7.5	CVE-2020-24000 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- forticlient	An improper authorization vulnerability [CWE-285] in FortiClient for Windows versions 7.0.1 and below and 6.4.2 and below may allow a local unprivileged attacker to escalate their privileges to SYSTEM via the named pipe responsible for Forticlient updates.	2021-11-02	7.2	CVE-2021-36183 CONFIRM
fortinet -- fortiweb	A stack-based buffer overflow in Fortinet FortiWeb version 6.4.0, version 6.3.15 and below, 6.2.5 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests	2021-11-02	7.5	CVE-2021-36186 CONFIRM
hp -- futuresmart_3	Certain HP Enterprise LaserJet, HP LaserJet Managed, HP Enterprise PageWide, HP PageWide Managed products may be vulnerable to potential buffer overflow.	2021-11-03	7.5	CVE-2021-39238 MISC
hp -- ilo_amplifier_pack	A remote unauthenticated directory traversal security vulnerability has been identified in HPE iLO Amplifier Pack versions 1.80, 1.81, 1.90 and 1.95. The vulnerability could be remotely exploited to allow an unauthenticated user to run arbitrary code leading complete impact to confidentiality, integrity, and availability of the iLO Amplifier Pack appliance.	2021-11-01	10	CVE-2021-29212 MISC MISC
hp -- laserjet_pro_j8h60a_firmware	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow a Denial of Service on the device.	2021-11-01	7.8	CVE-2021-3704 MISC
hp -- laserjet_pro_j8h61a_firmware	Potential security vulnerabilities have been discovered on a certain HP LaserJet Pro printer that may allow an unauthorized user to reconfigure, reset the device.	2021-11-01	10	CVE-2021-3705 MISC
hpe -- proliant_microserver_gen10_plus_firmware	A potential local bypass of security restrictions vulnerability has been identified in HPE ProLiant DL20 Gen10, HPE ProLiant ML30 Gen10, and HPE ProLiant MicroServer Gen10 Plus server's system ROMs prior to version 2.52. The vulnerability could be locally exploited to cause disclosure of sensitive information, denial of service (DoS), and/or compromise system integrity.	2021-11-01	7.2	CVE-2021-29213 MISC
json-ptr_project -- json-ptr	This affects the package json-ptr before 3.0.0. A type confusion vulnerability can lead to a bypass of CVE-2020-7766 when the user-provided keys used in the pointer parameter are arrays.	2021-11-03	7.5	CVE-2021-23509 MISC MISC MISC MISC MISC
jsonpointer_project -- jsonpointer	This affects all versions of package json-pointer. A type confusion vulnerability can lead to a bypass of CVE-2020-7709 when the pointer components are arrays.	2021-11-03	7.5	CVE-2021-23820 MISC MISC MISC
jsonpointer_project -- jsonpointer	This affects the package jsonpointer before 5.0.0. A type confusion vulnerability can lead to a bypass of a previous Prototype Pollution fix when the pointer components are arrays.	2021-11-03	7.5	CVE-2021-23807 MISC MISC MISC MISC
linux -- linux_kernel	An issue was discovered in net/tipc/crypto.c in the Linux kernel before 5.14.16. The Transparent Inter-Process Communication (TIPC) functionality allows remote attackers to exploit insufficient validation of user-supplied sizes for the MSG_CRYPTO message type.	2021-11-02	7.5	CVE-2021-43267 MISC MISC FEDORA FEDORA
linux_network_project -- linux_network_project	Buffer overflow vulnerability in Renleilei1992 Linux_Network_Project 1.0, allows attackers to execute arbitrary code, via the password field.	2021-11-03	7.5	CVE-2020-23679 MISC
mahara -- mahara	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, the account associated with a web services token is vulnerable to being exploited and logged into, resulting in information disclosure (at a minimum) and often escalation of privileges.	2021-11-03	7.5	CVE-2021-40849 MISC MISC
online_food_ordering_system_project -- online_food_ordering_system	Remote Code Exection (RCE) vulnerability exists in Sourcecodester Online Food Ordering System 2.0 via a maliciously crafted PHP file that bypasses the image upload filters.	2021-10-29	7.5	CVE-2021-41644 MISC
online_reviewer_system_project -- online_reviewer_system	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Online Reviewer System 1.0 by uploading a maliciously crafted PHP file that bypasses the image upload filters..	2021-10-29	7.5	CVE-2021-41646 MISC
pharmacy_point_of_sale_system_project -- pharmacy_point_of_sale_system	An SQL Injection vulnerabilty exists in the oretnom23 Pharmacy Point of Sale System 1.0 in the login function in actions.php.	2021-10-29	7.5	CVE-2021-41676 MISC MISC
phone_shop_sales_management_system_project -- phone_shop_sales_management_system	Phone Shop Sales Managements System using PHP with Source Code 1.0 is vulnerable to authentication bypass which leads to account takeover of the admin.	2021-11-02	7.5	CVE-2021-36560 MISC MISC
phpok -- phpok	Buffer overflow vulnerability in framework/init.php in qinggan phpok 5.1, allows attackers to execute arbitrary code.	2021-11-02	7.5	CVE-2020-18440 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
simple_cashiering_system_project -- simple_cashiering_system	Multiple SQL Injection vulnerabilities exist in Sourcecodester Simple Cashiering System (POS) 1.0 via the (1) Product Code in the pos page in cashiering. (2) id parameter in manage_products and the (3) t paramater in actions.php.	2021-11-03	7.5	CVE-2021-41492 MISC
simple_subscription_website_project -- simple_subscription_website	SQL Injection vulnerability exists in Sourcecodester. Simple Subscription Website 1.0. via the login.	2021-11-03	7.5	CVE-2021-43140 MISC
spacewalk_project -- spacewalk	Spacewalk 2.10, and derivatives such as Uyuni 2021.08, allows code injection. rhn-config-satellite.pl doesn't sanitize the configuration filename used to append Spacewalk-specific key-value pair. The script is intended to be run by the tomcat user account with Sudo, according to the installation setup. This can lead to the ability of an attacker to use --option to append arbitrary code to a root-owned file that eventually will be executed by the system. This is fixed in Uyuni spacewalk-admin 4.3.2-1.	2021-11-01	9.3	CVE-2021-40348 MISC CONFIRM
symonics -- libmysofa	libmysofa is vulnerable to Heap-based Buffer Overflow	2021-10-29	7.5	CVE-2021-3756 MISC CONFIRM
tendacn -- ac10u_firmware	Stack-based buffer overflow in Tenda AC-10U AC1200 Router US_AC10UV1.0RTL_V15.03.06.48_multi_TDE01 allows remote attackers to execute arbitrary code via the timeZone parameter to goform/SetSysTimeCfg.	2021-10-29	7.5	CVE-2020-22079 MISC MISC
thunderdome -- planning_poker	Thunderdome is an open source agile planning poker tool in the theme of Battling for points. In affected versions there is an LDAP injection vulnerability which affects instances with LDAP authentication enabled. The provided username is not properly escaped. This issue has been patched in version 1.16.3. If users are unable to update they should disable the LDAP feature if in use.	2021-11-02	7.5	CVE-2021-41232 CONFIRM MISC MISC
unicode -- unicode	An issue was discovered in the Bidirectional Algorithm in the Unicode Specification through 14.0. It permits the visual reordering of characters via control sequences, which can be used to craft source code that renders different logic than the logical ordering of tokens ingested by compilers and interpreters. Adversaries can leverage this to encode source code for compilers accepting Unicode such that targeted vulnerabilities are introduced invisibly to human reviewers.	2021-11-01	7.5	CVE-2021-42574 MISC MISC MLIST MLIST MLIST MLIST MLIST FEDORA FEDORA
unicode -- unicode	An issue was discovered in the character definitions of the Unicode Specification through 14.0. The specification allows an adversary to produce source code identifiers such as function names using homoglyphs that render visually identical to a target identifier. Adversaries can leverage this to inject code via adversarial identifier definitions in upstream software dependencies invoked deceptively in downstream software.	2021-11-01	7.5	CVE-2021-42694 MISC MISC MLIST MLIST
vtimecn -- 188jianzhan	SQL Injection vulnerability in 188Jianzhan v2.1.0, allows attackers to execute arbitrary code and gain escalated privileges, via the username parameter to login.php.	2021-11-02	7.5	CVE-2020-23685 MISC
zohocorp -- manageengine_applications_manager	An issue was found in /showReports.do Zoho ManageEngine Applications Manager up to 14550, allows attackers to gain escalated privileges via the resourceid parameter.	2021-11-03	7.5	CVE-2020-24743 MISC
zohocorp -- manageengine_log360	ManageEngine Log360 Builds < 5235 are affected by an improper access control vulnerability allowing database configuration overwrite. An unauthenticated remote attacker can send a specially crafted message to Log360 to change its backend database to an attacker-controlled database and to force Log360 to restart. An attacker can leverage this vulnerability to achieve remote code execution by replacing files executed by Log360 on startup.	2021-11-01	7.5	CVE-2021-20136 MISC

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
akka -- http_server	Akka HTTP 10.1.x and 10.2.x before 10.2.7 can encounter stack exhaustion while parsing HTTP headers, which allows a remote attacker to conduct a Denial of Service attack by sending a User-Agent header with deeply nested comments.	2021-11-02	5	CVE-2021-42697 MISC MISC MISC
alibaba -- druid	In Druid 1.2.3, visiting the path with parameter in a certain function can lead to directory traversal.	2021-11-03	5	CVE-2021-33800 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
antennahouse -- office_server_document_converter	Office Server Document Converter V7.2MR4 and earlier and V7.1MR7 and earlier allows a remote unauthenticated attacker to conduct an XML External Entity (XXE) attack to cause a denial of service (DoS) condition by processing a specially crafted XML document.	2021-11-01	5	CVE-2021-20838 MISC MISC
antennahouse -- office_server_document_converter	Office Server Document Converter V7.2MR4 and earlier and V7.1MR7 and earlier allows a remote unauthenticated attacker to conduct an XML External Entity (XXE) attack to cause a denial of service (DoS) condition to the other servers by processing a specially crafted XML document.	2021-11-01	4.3	CVE-2021-20839 MISC MISC
apache -- dolphinscheduler	In Apache DolphinScheduler before 1.3.6 versions, authorized users can use SQL injection in the data source center. (Only applicable to MySQL data source with internal login account password)	2021-11-01	6	CVE-2021-27644 MISC MLIST MLIST
apache -- mina	In Apache MINA, a specifically crafted, malformed HTTP request may cause the HTTP Header decoder to loop indefinitely. The decoder assumed that the HTTP Header begins at the beginning of the buffer and loops if there is more data than expected. Please update MINA to 2.1.5 or greater.	2021-11-01	4.3	CVE-2021-41973 MISC MLIST MLIST
apache -- traffic_server	Improper input validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and 9.0.0 to 9.0.1.	2021-11-03	5	CVE-2021-37148 MISC
apache -- traffic_server	Improper input validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and 9.0.0 to 9.1.0.	2021-11-03	5	CVE-2021-37147 MISC
apache -- traffic_server	Improper Input Validation vulnerability in header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 8.1.2 and 9.0.0 to 9.1.0.	2021-11-03	5	CVE-2021-37149 MISC
apache -- traffic_server	Improper Input Validation vulnerability in accepting socket connections in Apache Traffic Server allows an attacker to make the server stop accepting new connections. This issue affects Apache Traffic Server 5.0.0 to 9.1.0.	2021-11-03	5	CVE-2021-41585 MISC
apache -- traffic_server	Improper Authentication vulnerability in TLS origin verification of Apache Traffic Server allows for man in the middle attacks. This issue affects Apache Traffic Server 8.0.0 to 8.0.8.	2021-11-03	6.8	CVE-2021-38161 MISC
artica -- pandora_fms	With an admin account, the .htaccess file in Artica Pandora FMS <=755 can be overwritten with the File Manager component. The new .htaccess file contains a Rewrite Rule with a type definition. A normal PHP file can be uploaded with this new "file type" and the code can be executed with an HTTP request.	2021-11-03	4.6	CVE-2021-36697 MISC MISC MISC
atlassian -- data_center	Affected versions of Atlassian Jira Server and Data Center allow a remote attacker who has had their access revoked from Jira Service Management to enable and disable Issue Collectors on Jira Service Management projects via an Improper Authentication vulnerability in the /secure/ViewCollectors endpoint. The affected versions are before version 8.19.1.	2021-11-03	5	CVE-2021-41312 MISC
atlassian -- jira_software_data_center	Affected versions of Atlassian Jira Server and Data Center allow authenticated but non-admin remote attackers to edit email batch configurations via an Improper Authorization vulnerability in the /secure/admin/ConfigureBatching!default.jspa endpoint. The affected versions are before version 8.21.0.	2021-11-01	4	CVE-2021-41313 N/A
atlassian -- jira_software_data_center	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in the Associated Projects feature (/secure/admin/AssociatedProjectsForCustomField.jspa). The affected versions are before version 8.5.19, from version 8.6.0 before 8.13.11, and from version 8.14.0 before 8.19.1.	2021-11-01	4.3	CVE-2021-41310 MISC
automatorwp -- automatorwp	The AutomatorWP WordPress plugin before 1.7.6 does not perform capability checks which allows users with Subscriber roles to enumerate automations, disclose title of private posts or user emails, call functions, or perform privilege escalation via Ajax actions.	2021-11-01	6.5	CVE-2021-24717 MISC
baijiacms_project -- baijiacms	A directory traversal vulnerability in the component system/manager/class/web/database.php was discovered in Baijiacms V4 which allows attackers to arbitrarily delete folders on the server via the "id" parameter.	2021-10-29	4	CVE-2020-25873 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bootstrap_table_project -- bootstrap_table	This affects all versions of package bootstrap-table. A type confusion vulnerability can lead to a bypass of input sanitization when the input provided to the escapeHTML function is an array (instead of a string) even if the escape attribute is set.	2021-11-03	4.3	CVE-2021-23472 MISC MISC MISC MISC MISC MISC
budget_and_expense_tracker_system_project -- budget_and_expense_tracker_system	Remote Code Execution (RCE) vulnerability exists in Sourcecodester Budget and Expense Tracker System 1.0 that allows a remote malicious user to inject arbitrary code via the image upload field. .	2021-10-29	6.5	CVE-2021-41645 MISC
c-http_project -- c-http	Buffer overflow vulnerability in YotsuyaNight c-http v0.1.0, allows attackers to cause a denial of service via a long url request which is passed to the delimitedread function.	2021-11-02	5	CVE-2020-21574 MISC
chamilo -- chamilo_lms	Chamilo LMS version 1.11.10 contains an XSS vulnerability in the personal profile edition form, affecting the user him/herself and social network friends.	2021-11-03	4.3	CVE-2020-23126 MISC
cisco -- catalyst_pon_switch_cgp-ont-1p_firmware	Multiple vulnerabilities in the web-based management interface of the Cisco Catalyst Passive Optical Network (PON) Series Switches Optical Network Terminal (ONT) could allow an unauthenticated, remote attacker to perform the following actions: Log in with a default credential if the Telnet protocol is enabled Perform command injection Modify the configuration For more information about these vulnerabilities, see the Details section of this advisory.	2021-11-04	5	CVE-2021-40112 CISCO
cisco -- collaboration_meeting_rooms	A vulnerability in the web-based management interface of Cisco Webex Video Mesh could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious website. Attackers may use this type of vulnerability, known as an open redirect attack, as part of a phishing attack to persuade users to unknowingly visit malicious sites.	2021-11-04	5.8	CVE-2021-1500 CISCO
cisco -- collaboration_meeting_rooms	A vulnerability in Cisco Webex Video Mesh could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.	2021-11-04	4.3	CVE-2021-40115 CISCO
cisco -- common_services_platform_collecto	A vulnerability in the web-based management interface of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to access sensitive data on an affected system. This vulnerability exists because the application does not sufficiently protect sensitive data when responding to a specific API request. An attacker could exploit the vulnerability by sending a crafted HTTP request to the affected application. A successful exploit could allow the attacker to obtain sensitive information about the users of the application, including security questions and answers. To exploit this vulnerability an attacker would need valid Administrator credentials. Cisco expects to release software updates that address this vulnerability.	2021-11-04	4	CVE-2021-34774 CISCO
cisco -- umbrella	A vulnerability in the web-based dashboard of Cisco Umbrella could allow an authenticated, remote attacker to perform an email enumeration attack against the Umbrella infrastructure. This vulnerability is due to an overly descriptive error message on the dashboard that appears when a user attempts to modify their email address when the new address already exists in the system. An attacker could exploit this vulnerability by attempting to modify the user's email address. A successful exploit could allow the attacker to enumerate email addresses of users in the system.	2021-11-04	4	CVE-2021-40126 CISCO

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the targeted user. These actions could include modifying the device configuration and deleting (but not creating) user accounts.	2021-11-04	4.3	CVE-2021-34773 CISCO
cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P), and Cisco Unity Connection could allow an authenticated, remote attacker to access sensitive data on an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the affected system.	2021-11-04	4	CVE-2021-34701 CISCO
cisco -- webex_meetings	A vulnerability in the account activation feature of Cisco Webex Meetings could allow an unauthenticated, remote attacker to send an account activation email with an activation link that points to an arbitrary domain. This vulnerability is due to insufficient validation of user-supplied parameters. An attacker could exploit this vulnerability by sending a crafted HTTP request to the account activation page of Cisco Webex Meetings. A successful exploit could allow the attacker to send to any recipient an account activation email that contains a tampered activation link, which could direct the user to an attacker-controlled website.	2021-11-04	5	CVE-2021-40128 CISCO
connections-pro -- connections_business_directory	The Connections Business Directory WordPress plugin before 9.7 does not validate or sanitise some connections' fields, which could lead to a CSV injection issue	2021-11-01	6	CVE-2020-36503 MISC MISC
d-link -- dir-868lw_firmware	Several web interfaces in D-Link DIR-868LW 1.12b have no authentication requirements for access, allowing for attackers to obtain users' DNS query history.	2021-10-31	5	CVE-2021-33259 MISC MISC MISC MISC
datalust -- seq.app.emailplus	Datalust Seq.App.EmailPlus (aka seq-app-htmlemail) 3.1.0-dev-00148, 3.1.0-dev-00170, and 3.1.0-dev-00176 can use cleartext SMTP on port 25 in some cases where encryption on port 465 was intended.	2021-11-02	5	CVE-2021-43270 MISC
delete_all_comments_easily_project -- delete_all_comments_easily	The Delete All Comments Easily WordPress plugin through 1.3 is lacking Cross-Site Request Forgery (CSRF) checks, which could result in an unauthenticated attacker making a logged in admin delete all comments from the blog.	2021-11-01	4.3	CVE-2020-36505 MISC MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior runs by default on HTTP, which may allow an attacker to be positioned between the traffic and perform a machine-in-the-middle attack to access information without authorization.	2021-11-03	4.3	CVE-2021-38418 MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior stores sensitive information in cleartext, which may allow an attacker to have extensive access to the application directory and escalate privileges.	2021-11-03	4.6	CVE-2021-38422 MISC
deltaww -- dialink	The tag interface of Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to an attacker injecting formulas into the tag data. Those formulas may then be executed when it is opened with a spreadsheet application.	2021-11-03	6.8	CVE-2021-38424 MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior default permissions give extensive permissions to low-privileged user accounts, which may allow an attacker to modify the installation directory and upload malicious files.	2021-11-03	4.6	CVE-2021-38420 MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior insecurely loads libraries, which may allow an attacker to use DLL hijacking and takeover the system where the software is installed.	2021-11-03	4.4	CVE-2021-38416 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dhis2 -- dhis_2	DHIS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL injection security vulnerability has been found in specific versions of DHIS2. This vulnerability affects the API endpoints for /api/trackedEntityInstances and api/events in DHIS2. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance. There are no known exploits of the security vulnerabilities addressed by these patch releases. However, we strongly recommend that all DHIS2 implementations using versions 2.32, 2.33, 2.34, 2.35 and 2.36 install these patches as soon as possible. There is no straightforward known workaround for DHIS2 instances using the Tracker functionality other than upgrading the affected DHIS2 server to one of the patches in which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to block all network access to POST to the /api/trackedEntityInstance and /api/events endpoints as a temporary workaround while waiting to upgrade.	2021-11-01	6.5	CVE-2021-41187 CONFIRM
dhis2 -- dhis_2	DHIS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL Injection vulnerability in the Tracker component in DHIS2 Server allows authenticated remote attackers to execute arbitrary SQL commands via unspecified vectors. This vulnerability affects the `/api/trackedEntityInstances` and `/api/trackedEntityInstances/query` API endpoints in all DHIS2 versions 2.34, 2.35, and 2.36. It also affects versions 2.32 and 2.33 which have reached _end of support_ - exceptional security updates have been added to the latest *end of support* builds for these versions. Versions 2.31 and older are unaffected. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. The vulnerability is not exposed to a non-malicious user - the vulnerability requires a conscious attack to be exploited. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance. There are no known exploits of the security vulnerabilities addressed by these patch releases. Security patches are available in DHIS2 versions 2.32-EOS, 2.33-EOS, 2.34.7, 2.35.7, and 2.36.4. There is no straightforward known workaround for DHIS2 instances using the Tracker functionality other than upgrading the affected DHIS2 server to one of the patches in which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to block all network access to POST to the `/api/trackedEntityInstances`, and `/api/trackedEntityInstances/query` endpoints as a temporary workaround while waiting to upgrade.	2021-10-29	6.5	CVE-2021-39179 CONFIRM MISC MISC
e-negosyo_system_project -- e-negosyo_system	A Remote Code Execution (RCE) vulnerabilty exists in Sourcecodester E-Negosyo System 1.0 in /admin/produts/controller.php via the doInsert function, which validates images with getImageSizei. .	2021-10-29	6.5	CVE-2021-41675 MISC
ec_cloud_e-commerce_system_project -- ec_cloud_e-commerce_system	EC Cloud E-Commerce System v1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily add admin accounts via /admin.html?do=user&act=add.	2021-11-04	4.3	CVE-2020-21139 MISC
ed01-cms_project -- ed01-cms	ED01-CMS v1.0 was discovered to contain a reflective cross-site scripting (XSS) vulnerability in the component sposts.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the Post title or Post content fields.	2021-11-03	4.3	CVE-2020-18259 MISC
elkarbackup -- elkarbackup	Cross Site Scripting (XSS) vulnerability in ElkarBackup 1.3.3, allows attackers to execute arbitrary code via the name parameter to the add client feature.	2021-11-02	4.3	CVE-2020-35249 MISC
ericsson -- network_location_mps_gmpc21	In Ericsson Network Location MPS GMPC21, it is possible to creates a new admin user with a SQL Query for file_name in the export functionality.	2021-11-03	6.5	CVE-2021-43338 MISC MISC
fimer -- aurora_vision	An issue was discovered in Fimer Aurora Vision before 2.97.10. An attacker can (in the WebUI) obtain plant information without authentication by reading the response of APIs from a kiosk view of a plant.	2021-11-03	4.3	CVE-2021-33210 MISC MISC
fimer -- aurora_vision	An issue was discovered in Fimer Aurora Vision before 2.97.10. The response to a failed login attempt discloses whether the username or password is wrong, helping an attacker to enumerate usernames. This can make a brute-force attack easier.	2021-11-03	5	CVE-2021-33209 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
flat_preloader_project -- flat_preloader	The Flat Preloader WordPress plugin before 1.5.4 does not enforce nonce checks when saving its settings, as well as does not sanitise and escape them, which could allow attackers to a make logged in admin change them with a Cross-Site Scripting payload (triggered either in the frontend or backend depending on the payload)	2021-11-01	5	CVE-2021-24685 MISC
fluentd -- fluentd	Fluentd collects events from various data sources and writes them to files to help unify logging infrastructure. The parser_apache2 plugin in Fluentd v0.14.14 to v1.14.1 suffers from a regular expression denial of service (ReDoS) vulnerability. A broken apache log with a certain pattern of string can spend too much time in a regular expression, resulting in the potential for a DoS attack. This issue is patched in version 1.14.2 There are two workarounds available. Either don't use parser_apache2 for parsing logs (which cannot guarantee generated by Apache), or put patched version of parser_apache2.rb into /etc/fluent/plugin directory (or any other directories specified by the environment variable `FLUENT_PLUGIN` or `--plugin` option of fluentd).	2021-10-29	5	CVE-2021-41186 MISC MISC CONFIRM
fortinet -- fortiadc	A cleartext storage of sensitive information in GUI in FortiADC versions 5.4.3 and below, 6.0.0 and below may allow a remote authenticated attacker to retrieve some sensitive information such as users LDAP passwords and RADIUS shared secret by deobfuscating the passwords entry fields.	2021-11-02	4	CVE-2020-15935 CONFIRM
fortinet -- fortimanager	An improper access control vulnerability [CWE-284] in FortiManager versions 6.4.4 and 6.4.5 may allow an authenticated attacker with a restricted user profile to modify the VPN tunnel status of other VDOMs using VPN Manager.	2021-11-02	4	CVE-2021-26107 CONFIRM MISC
fortinet -- fortios	An improper validation of certificate with host mismatch [CWE-297] vulnerability in FortiOS versions 6.4.6 and below may allow the connection to a malicious LDAP server via options in GUI, leading to disclosure of sensitive information, such as AD credentials.	2021-11-02	4.3	CVE-2021-41019 CONFIRM
fortinet -- fortiportal	Multiple uncontrolled resource consumption vulnerabilities in the web interface of FortiPortal before 6.0.6 may allow a single low-privileged user to induce a denial of service via multiple HTTP requests.	2021-11-02	4	CVE-2021-32595 CONFIRM
fortinet -- fortiportal	An improper restriction of XML external entity reference vulnerability in the parser of XML responses of FortiPortal before 6.0.6 may allow an attacker who controls the producer of XML reports consumed by FortiPortal to trigger a denial of service or read arbitrary files from the underlying file system by means of specifically crafted XML documents.	2021-11-02	6.4	CVE-2021-36172 CONFIRM
fortinet -- fortiportal	Multiple uncontrolled resource consumption vulnerabilities in the web interface of FortiPortal before 6.0.6 may allow a single low-privileged user to induce a denial of service via multiple HTTP requests.	2021-11-02	4.3	CVE-2021-36176 CONFIRM
fortinet -- fortiportal	A memory allocation with excessive size value vulnerability in the license verification function of FortiPortal before 6.0.6 may allow an attacker to perform a denial of service attack via specially crafted license blobs.	2021-11-02	5	CVE-2021-36174 CONFIRM
fortinet -- fortisiem	A improper privilege management in Fortinet FortiSIEM Windows Agent version 4.1.4 and below allows attacker to execute privileged code or commands via powershell scripts	2021-11-02	4.6	CVE-2021-41022 CONFIRM
fortinet -- fortiweb	A uncontrolled resource consumption in Fortinet FortiWeb version 6.4.0, version 6.3.15 and below, 6.2.5 and below allows attacker to cause a denial of service for webserver daemon via crafted HTTP requests	2021-11-02	5	CVE-2021-36187 CONFIRM
fortinet -- fortiwlm	A improper neutralization of Special Elements used in an SQL Command ('SQL Injection') in Fortinet FortiWLM version 8.6.1 and below allows attacker to disclosure device, users and database information via crafted HTTP requests.	2021-11-02	4	CVE-2021-36184 CONFIRM
fortinet -- fortiwlm	A improper neutralization of special elements used in an OS command ('OS Command Injection') in Fortinet FortiWLM version 8.6.1 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests.	2021-11-02	6.5	CVE-2021-36185 CONFIRM
frogcms_project -- frogcms	A vulnerability exists within the FileManagerController.php function in FrogCMS 0.9.5 which allows an attacker to perform a directory traversal attack via a GET request urlencode parameter.	2021-10-29	4	CVE-2020-25872 MISC
getsymphony -- symphony	A XML External Entity (XXE) vulnerability was discovered in symphony\lib\toolkit\class.xmlelement.php in Symphony 2.7.10 which can lead to an information disclosure or denial of service (DOS).	2021-10-31	6.4	CVE-2020-25912 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
gilcc_project -- gilcc	Buffer overflow vulnerability in function src_parser_trans_stage_1_2_3 trgil gilcc before commit 803969389ca9c06237075a7f8eeb1a19e6651759, allows attackers to cause a denial of service.	2021-11-02	5	CVE-2020-21572 MISC MISC
google -- angle	Out of bounds read in ANGLE allowed a remote attacker to obtain sensitive data via a crafted HTML page.	2021-11-02	4.3	CVE-2020-16048 MISC
google -- chrome	Inappropriate implementation in Sandbox in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially bypass site isolation via Windows.	2021-11-02	4.3	CVE-2021-37980 MISC MISC FEDORA
google -- chrome	Inappropriate implementation in Blink in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to abuse content security policy via a crafted HTML page.	2021-11-02	4.3	CVE-2021-37989 MISC MISC
google -- chrome	Inappropriate implementation in iFrame Sandbox in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2021-11-02	4.3	CVE-2021-37994 MISC MISC
google -- chrome	Inappropriate implementation in WebApp Installer in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially overlay and spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2021-11-02	4.3	CVE-2021-37995 MISC MISC
google -- chrome	Insufficient validation of untrusted input Downloads in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to bypass navigation restrictions via a malicious file.	2021-11-02	4.3	CVE-2021-37996 MISC MISC
google -- chrome	Insufficient policy enforcement in USB in Google Chrome on Windows prior to 67.0.3396.62 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page.	2021-11-02	4.3	CVE-2018-6125 MISC
google -- chrome	Inappropriate implementation in WebView in Google Chrome on Android prior to 95.0.4638.54 allowed a remote attacker to leak cross-origin data via a crafted app.	2021-11-02	4.3	CVE-2021-37990 MISC MISC
google -- chrome	Type confusion in WebAssembly in Google Chrome prior to 66.0.3359.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2018-6122 MISC
google -- chrome	Use after free in Incognito in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37982 MISC MISC
google -- chrome	Heap buffer overflow in Blink in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37978 MISC MISC FEDORA
google -- chrome	Use after free in Dev Tools in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37983 MISC MISC
google -- chrome	Heap buffer overflow in PDFium in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37984 MISC MISC
google -- chrome	Race in V8 in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	5.1	CVE-2021-37991 MISC MISC
google -- chrome	Use after free in V8 in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had convinced a user to allow for connection to debugger to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37985 MISC MISC
google -- chrome	Heap buffer overflow in Skia in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37981 MISC MISC
google -- chrome	Heap buffer overflow in Settings in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to engage with Dev Tools to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37986 MISC MISC
google -- chrome	Use after free in Garbage Collection in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37977 MISC MISC FEDORA
google -- chrome	Use after free in Network APIs in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37987 MISC MISC
google -- chrome	Use after free in Profiles in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who convinced a user to engage in specific gestures to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37988 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Out of bounds read in WebAudio in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37992 MISC MISC
google -- chrome	Use after free in PDF Accessibility in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37993 MISC MISC
google -- chrome	Use after free in ANGLE in Google Chrome prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2021-11-02	6.8	CVE-2020-6492 MISC MISC
google -- chrome	heap buffer overflow in WebRTC in Google Chrome prior to 94.0.4606.81 allowed a remote attacker who convinced a user to browse to a malicious website to potentially exploit heap corruption via a crafted HTML page.	2021-11-02	6.8	CVE-2021-37979 MISC MISC FEDORA
grafana -- grafana	Grafana is an open-source platform for monitoring and observability. In affected versions if an attacker is able to convince a victim to visit a URL referencing a vulnerable page, arbitrary JavaScript content may be executed within the context of the victim's browser. The user visiting the malicious link must be unauthenticated and the link must be for a page that contains the login button in the menu bar. The url has to be crafted to exploit AngularJS rendering and contain the interpolation binding for AngularJS expressions. AngularJS uses double curly braces for interpolation binding: {{ }} ex: {{constructor.constructor(â€˜alert(1)â€™)()}}. When the user follows the link and the page renders, the login button will contain the original link with a query parameter to force a redirect to the login page. The URL is not validated and the AngularJS rendering engine will execute the JavaScript expression contained in the URL. Users are advised to upgrade as soon as possible. If for some reason you cannot upgrade, you can use a reverse proxy or similar to block access to block the literal string {{ in the path.	2021-11-03	4.3	CVE-2021-41174 MISC MISC MISC CONFIRM
hangfire -- hangfire	Hangfire is an open source system to perform background job processing in a .NET or .NET Core applications. No Windows Service or separate process required. Dashboard UI in Hangfire.Core uses authorization filters to protect it from showing sensitive data to unauthorized users. By default when no custom authorization filters specified, `LocalRequestsOnlyAuthorizationFilter` filter is being used to allow only local requests and prohibit all the remote requests to provide sensible, protected by default settings. However due to the recent changes, in version 1.7.25 no authorization filters are used by default, allowing remote requests to succeed. If you are using `UseHangfireDashboard` method with default `DashboardOptions.Authorization` property value, then your installation is impacted. If any other authorization filter is specified in the `DashboardOptions.Authorization` property, the you are not impacted. Patched versions (1.7.26) are available both on Nuget.org and as a tagged release on the github repo. Default authorization rules now prohibit remote requests by default again by including the `LocalRequestsOnlyAuthorizationFilter` filter to the default settings. Please upgrade to the newest version in order to mitigate the issue. For users who are unable to upgrade it is possible to mitigate the issue by using the `LocalRequestsOnlyAuthorizationFilter` explicitly when configuring the Dashboard UI.	2021-11-02	5	CVE-2021-41238 MISC CONFIRM
hashthemes -- hashthemes_demo_importer	The Hashthemes Demo Importer Plugin <= 1.1.1 for WordPress contained several AJAX functions which relied on a nonce which was visible to all logged-in users for access control, allowing them to execute a function that truncated nearly all database tables and removed the contents of wp-content/uploads.	2021-11-01	5.5	CVE-2021-39333 MISC
hp -- hp_smart	HP Print and Scan Doctor, an application within the HP Smart App for Windows, is potentially vulnerable to local elevation of privilege.	2021-11-01	4.6	CVE-2021-3440 MISC
hp -- print_and_scan_doctor	HP Print and Scan Doctor may potentially be vulnerable to local elevation of privilege.	2021-11-03	4.6	CVE-2020-6931 MISC
htmldoc_project -- htmldoc	Buffer overflow vulnerability in htmldoc before 1.9.12, allows attackers to cause a denial of service via a crafted BMP image to image_load_bmp.	2021-11-03	4.3	CVE-2021-40985 MISC MISC
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 207123.	2021-11-02	6.8	CVE-2021-29888 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- infosphere_information_server	IBM InfoSphere Data Flow Designer (IBM InfoSphere Information Server 11.7) is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 201302.	2021-11-02	5.5	CVE-2021-29738 XF CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 could allow an attacker to obtain sensitive information due to a insecure third party domain access vulnerability. IBM X-Force ID: 206572.	2021-11-02	5	CVE-2021-29875 XF CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Data Flow Designer Engine (IBM InfoSphere Information Server 11.7) component has improper validation of the REST API server certificate. IBM X-Force ID: 201301.	2021-11-02	5	CVE-2021-29737 XF CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 211402.	2021-11-02	6.4	CVE-2021-38948 CONFIRM XF
image-processing_project -- image-processing	An issue was discoverered in in abhijitnathwani image-processing v0.1.0, allows local attackers to cause a denial of service via a crafted image file.	2021-11-02	4.3	CVE-2020-21573 MISC
imagesourcecontrol -- image_source_control	The Image Source Control WordPress plugin before 2.3.1 allows users with a role as low as Contributor to change arbitrary post meta fields of arbitrary posts (even those they should not be able to edit)	2021-11-01	4	CVE-2021-24781 MISC CONFIRM
jenkins -- jenkins	The agent-to-controller security check FilePath#reading(FileVisitor) in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not reject any operations, allowing users to have unrestricted read access using certain operations (creating archives, FilePath#copyRecursiveTo).	2021-11-04	5	CVE-2021-21688 CONFIRM
kodi -- kodi	Buffer overflow vulnerability in Kodi xbmc up to 19.0, allows attackers to cause a denial of service due to improper length of values passed to istream.	2021-11-01	4.3	CVE-2021-42917 MISC MISC MISC MISC
kubernetes -- ingress-nginx	A security issue was discovered in ingress-nginx where a user that can create or update ingress objects can use the custom snippets feature to obtain all secrets in the cluster.	2021-10-29	5.5	CVE-2021-25742 MLIST CONFIRM
learndash -- learndash	The LearnDash LMS WordPress plugin before 2.5.4 does not have any authorisation and validation of the file to be uploaded in the learndash_assignment_process_init() function, which could allow unauthenticated users to upload arbitrary files to the web server	2021-11-01	5	CVE-2018-25019 MISC MISC
libiec_iccp_mod_project -- libiec_iccp_mod	Buffer overflow vulnerability in fcovatti libiec_iccp_mod v1.5, allows attackers to cause a denial of service via an unexpected packet while trying to connect.	2021-11-02	5	CVE-2020-20657 MISC
libiec_iccp_mod_project -- libiec_iccp_mod	Buffer overflow vulnerability in fcovatti libiec_iccp_mod v1.5, allows attackers to cause a denail of service when trying to calloc an unexpectiedly large space.	2021-11-02	5	CVE-2020-20658 MISC
librenms -- librenms	LibreNMS through 21.10.2 allows XSS via a widget title.	2021-11-03	4.3	CVE-2021-43324 MISC
libxls_project -- libxls	An issue was discoverered in in function xls_getWorkSheet in xls.c in libxls 1.6.2, allows attackers to cause a denial of service, via a crafted XLS file.	2021-11-03	4.3	CVE-2021-27836 MISC
linux -- linux_kernel	A vulnerability was found in Linux kernel, where a use-after-frees in nouveau's postclose() handler could happen if removing device (that is not common to remove video card physically without power-off, but same happens if "unbind" the driver).	2021-11-03	4.7	CVE-2020-27820 MISC MISC MISC MISC
linux -- linux_kernel	Insufficient data validation in waitid allowed an user to escape sandboxes on Linux.	2021-11-02	4.6	CVE-2017-5123 MISC MISC
llhttp -- llhttp	The parse function in llhttp < 2.1.4 and < 6.0.6. ignores chunk extensions when parsing the body of chunked requests. This leads to HTTP Request Smuggling (HRS) under certain conditions.	2021-11-03	5.8	CVE-2021-22960 MISC
mahara -- mahara	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, exporting collections via PDF export could lead to code execution via shell metacharacters in a collection name.	2021-11-02	4.6	CVE-2021-43266 MISC MISC
mahara -- mahara	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, exported CSV files could contain characters that a spreadsheet program could interpret as a command, leading to execution of a malicious string locally on a device, aka CSV injection.	2021-11-03	6.8	CVE-2021-40848 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mcafee -- data_loss_prevention_endpoint	SQL injection vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.7.100 allows a remote attacker logged into ePO as an administrator to inject arbitrary SQL into the ePO database through the user management section of the DLP ePO extension.	2021-11-01	6.5	CVE-2021-31849 MISC
modx -- modx_revolution	A XML External Entity (XXE) vulnerability was discovered in the modRestServiceRequest component in MODX CMS 2.7.3 which can lead to an information disclosure or denial of service (DOS).	2021-10-31	6.4	CVE-2020-25911 MISC MISC
mozilla -- firefox	Through use of reportValidity() and window.open(), a plain-text validation message could have been overlaid on another origin, leading to possible user confusion and spoofing attacks. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.	2021-11-03	4.3	CVE-2021-38497 MISC MISC MISC MISC
mozilla -- firefox	Firefox incorrectly accepted a newline in a HTTP/3 header, interpretting it as two separate headers. This allowed for a header splitting attack against servers using HTTP/3. This vulnerability affects Firefox < 91.0.1 and Thunderbird < 91.0.1.	2021-11-03	5.8	CVE-2021-29991 MISC MISC
mozilla -- firefox	Firefox for Android allowed navigations through the \`intent://\` protocol, which could be used to cause crashes and UI spoofs. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92.	2021-11-03	5.8	CVE-2021-29993 MISC MISC
mozilla -- firefox	Mixed-content checks were unable to analyze opaque origins which led to some mixed content being loaded. This vulnerability affects Firefox < 92.	2021-11-03	4.3	CVE-2021-38491 MISC MISC
mozilla -- firefox	During operations on MessageTasks, a task may have been removed while it was still scheduled, resulting in memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93.	2021-11-03	6.8	CVE-2021-38496 MISC MISC MISC MISC MISC MISC
mozilla -- firefox	Mozilla developers reported memory safety bugs present in Firefox 92. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 93.	2021-11-03	6.8	CVE-2021-38499 MISC MISC
mozilla -- firefox	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93.	2021-11-03	6.8	CVE-2021-38500 MISC MISC MISC MISC MISC MISC
mozilla -- firefox	When delegating navigations to the operating system, Firefox would accept the \`mk\` scheme which might allow attackers to launch pages and execute scripts in Internet Explorer in unprivileged mode. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 92, Thunderbird < 91.1, Thunderbird < 78.14, Firefox ESR < 78.14, and Firefox ESR < 91.1.	2021-11-03	4.3	CVE-2021-38492 MISC MISC MISC MISC MISC MISC
mozilla -- firefox	Mozilla developers reported memory safety bugs present in Firefox 91 and Firefox ESR 78.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.14, Thunderbird < 78.14, and Firefox < 92.	2021-11-03	6.8	CVE-2021-38493 MISC MISC MISC MISC
mozilla -- firefox	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.	2021-11-03	6.8	CVE-2021-38501 MISC MISC MISC MISC
mozilla -- firefox	Mozilla developers reported memory safety bugs present in Firefox 91. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 92.	2021-11-03	6.8	CVE-2021-38494 MISC MISC
mozilla -- firefox	During process shutdown, a document could have caused a use-after-free of a languages service object, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.	2021-11-03	5	CVE-2021-38498 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mozilla -- firefox_esr	Mozilla developers reported memory safety bugs present in Thunderbird 78.13.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.1 and Firefox ESR < 91.1.	2021-11-03	6.8	CVE-2021-38495 MISC MISC MISC
mozilla -- thunderbird	Thunderbird ignored the configuration to require STARTTLS security for an SMTP connection. A MITM could perform a downgrade attack to intercept transmitted messages, or could take control of the authenticated session to execute SMTP commands chosen by the MITM. If an unprotected authentication method was configured, the MITM could obtain the authentication credentials, too. This vulnerability affects Thunderbird < 91.2.	2021-11-03	4.3	CVE-2021-38502 MISC MISC
mybb -- mybb	MyBB before 1.8.29 allows Remote Code Injection by an admin with the "Can manage settings?" permission. The Admin CP's Settings management module does not validate setting types correctly on insertion and update, making it possible to add settings of supported type "php" with PHP code, executed on Change Settings pages.	2021-11-04	6.5	CVE-2021-43281 CONFIRM
navercorp -- whale	Whale browser for iOS before 1.14.0 has an inconsistent user interface issue that allows an attacker to obfuscate the address bar which may lead to address bar spoofing.	2021-11-02	5	CVE-2021-33593 CONFIRM
netapp -- ontap_system_manager	Clustered Data ONTAP versions 9.6 and higher prior to 9.6P16, 9.7P16, 9.8P7 and 9.9.1P3 are susceptible to a vulnerability which could allow a remote attacker to cause a crash of the httpd server.	2021-11-01	5	CVE-2021-27005 MISC
nextscripts -- social_networks_auto_poster	The NextScripts: Social Networks Auto-Poster <= 4.3.20 WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the $_REQUEST['page'] parameter which is echoed out on inc/nxs_class_snap.php by supplying the appropriate value 'nxssnap-post' to load the page in $_GET['page'] along with malicious JavaScript in $_POST['page'].	2021-11-01	4.3	CVE-2021-38356 MISC
nsasoft -- spotauditor	An issue was discovered in Nsasoft US LLC SpotAuditor 5.3.5. The program can be crashed by entering 300 bytes char data into the "Key" or "Name" field while registering.	2021-11-02	5	CVE-2021-27722 MISC MISC
nvidia -- virtual_gpu	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a string provided by the guest OS may not be properly null terminated. The guest OS or attacker has no ability to push content to the plugin through this vulnerability, which may lead to information disclosure, data tampering, unauthorized code execution, and denial of service.	2021-10-29	4.6	CVE-2021-1120 CONFIRM
nvidia -- virtual_gpu	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where there is the potential to execute privileged operations by the guest OS, which may lead to information disclosure, data tampering, escalation of privileges, and denial of service	2021-10-29	4.6	CVE-2021-1118 CONFIRM
optinmonster -- optinmonster	The OptinMonster WordPress plugin is vulnerable to sensitive information disclosure and unauthorized setting updates due to insufficient authorization validation via the logged_in_or_has_api_key function in the ~/OMAPI/RestApi.php file that can used to exploit inject malicious web scripts on sites with the plugin installed. This affects versions up to, and including, 2.6.4.	2021-11-01	6.4	CVE-2021-39341 MISC MISC MISC
php-cms_project -- php-cms	PHP-CMS v1.0 was discovered to contain a SQL injection vulnerability in the component search.php via the search parameter. This vulnerability allows attackers to access sensitive database information.	2021-11-03	5	CVE-2020-18263 MISC
php-fusion -- phpfusion	Cross Site Scripting (XSS) vulnerability in infusions/member_poll_panel/poll_admin.php in PHP-Fusion 9.03.50, allows attackers to execute arbitrary code, via the polls feature.	2021-11-02	6.8	CVE-2020-23754 MISC MISC MISC
phpok -- phpok	Directory traversal vulnerability in qinggan phpok 5.1, allows attackers to disclose sensitive information, via the title parameter to admin.php.	2021-11-02	5	CVE-2020-18438 MISC
phpok -- phpok	An issue was discoverered in in function edit_save_f in framework/admin/tpl_control.php in qinggan phpok 5.1, allows attackers to write arbitrary files or get a shell.	2021-11-02	6.4	CVE-2020-18439 MISC
playtuber_project -- playtuber	An issue was discoverered in in customercentric-selling-poland PlayTube, allows authenticated attackers to execute arbitrary code via the purchace code to the config.php.	2021-11-03	6.5	CVE-2021-26786 MISC
portainer -- portainer	An Incorrect Access Control issue exists in all versions of Portainer.via an unauthorized access vulnerability. The vulnerability is also CNVD-2021-49547	2021-10-29	5	CVE-2021-41748 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
portainer -- portainer	An unauthorized access vulnerabiitly exists in all versions of Portainer, which could let a malicious user obtain sensitive information.	2021-10-29	5	CVE-2021-41874 MISC
publify_project -- publify	In Publify, 9.0.0.pre1 to 9.2.4 are vulnerable to Improper Access Control. “guest” role users can self-register even when the admin does not allow. This happens due to front-end restriction only.	2021-11-02	6.5	CVE-2021-25973 MISC MISC
pypi -- easyxml	The parseXML function in Easy-XML 0.5.0 was discovered to have a XML External Entity (XXE) vulnerability which allows for an attacker to expose sensitive data or perform a denial of service (DOS) via a crafted external entity entered into the XML content as input.	2021-10-31	6.4	CVE-2020-26705 MISC
radiustheme -- logo_slider_and_showcase	The Logo Slider and Showcase WordPress plugin before 1.3.37 allows Editor users to update the plugin's settings via the rtWLSSettings AJAX action because it uses a nonce for authorisation instead of a capability check.	2021-11-01	4	CVE-2021-24742 MISC
ranko -- rkcms	A vulnerability was discovered in the filename parameter in pathindex.php?r=cms-backend/attachment/delete&sub=&filename=../../../../111.txt&filetype=image/jpeg of the master version of RKCMS. This vulnerability allows for an attacker to perform a directory traversal via a crafted .txt file.	2021-10-29	4.3	CVE-2020-25881 MISC MISC MISC
replicated -- replicated_classic	An open redirect vulnerability exists in Replicated Classic versions prior to 2.53.1 that could lead to spoofing. To exploit this vulnerability, an attacker could send a link that has a specially crafted URL and convince the user to click the link, redirecting the user to an untrusted site.	2021-11-01	5.8	CVE-2021-43058 MISC
s-cart -- s-cart	S-Cart v6.4.1 and below was discovered to contain an arbitrary file upload vulnerability in the Editor module on the Admin panel. This vulnerability allows attackers to execute arbitrary code via a crafted IMG file.	2021-11-01	6.5	CVE-2021-38847 MISC
simple_subscription_website_project -- simple_subscription_website	Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Simple Subscription Website 1.0 via the id parameter in plan_application.	2021-11-03	4.3	CVE-2021-43141 MISC
siren -- investigate	In Siren Investigate before 11.1.4, when enabling the cluster feature of the Siren Alert application, TLS verifications are disabled globally in the Siren Investigate main process.	2021-11-02	6.8	CVE-2021-36794 MISC MISC MISC
solarwinds -- kiwi_syslog_server	A missing HTTP header (X-Frame-Options) in Kiwi Syslog Server has left customers vulnerable to click jacking. Clickjacking is an attack that occurs when an attacker uses a transparent iframe in a window to trick a user into clicking on an actionable item, such as a button or link, to another server in which they have an identical webpage. The attacker essentially hijacks the user activity intended for the original server and sends them to the other server. This is an attack on both the user and the server.	2021-10-29	4.3	CVE-2021-35237 MISC MISC
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager 3.x before 3.36.0 allows a remote authenticated attacker to potentially perform network enumeration via Server Side Request Forgery (SSRF).	2021-11-04	4	CVE-2021-43293 CONFIRM
sophos -- sophos_secure_workspace	A local attacker could bypass the app password using a race condition in Sophos Secure Workspace for Android before version 9.7.3115.	2021-10-30	4.4	CVE-2021-36808 CONFIRM
struktur -- libheif	Buffer overflow vulnerability in function convert_colorspace in heif_colorconversion.cc in libheif v1.6.2, allows attackers to cause a denial of service and disclose sensitive information, via a crafted HEIF file.	2021-11-03	5.8	CVE-2020-23109 MISC
stylishpricelist -- stylish_price_list	The Stylish Price List WordPress plugin before 6.9.0 does not perform capability checks in its spl_upload_ser_img AJAX action (available to both unauthenticated and authenticated users), which could allow unauthenticated users to upload images.	2021-11-01	5	CVE-2021-24757 MISC
stylishpricelist -- stylish_price_list	The Stylish Price List WordPress plugin before 6.9.1 does not perform capability checks in its spl_upload_ser_img AJAX action (available to authenticated users), which could allow any authenticated users, such as subscriber, to upload arbitrary images.	2021-11-01	4	CVE-2021-24770 MISC
sysaid -- sysaid	SysAid 20.4.74 allows XSS via the KeepAlive.jsp stamp parameter without any authentication.	2021-10-29	4.3	CVE-2021-31862 MISC MISC
tempura_project -- tempura	This affects the package tempura before 0.4.0. If the input to the esc function is of type object (i.e an array) it is returned without being escaped/sanitized, leading to a potential Cross-Site Scripting vulnerability.	2021-11-03	4.3	CVE-2021-23784 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tenable -- nessus	Nessus versions 8.15.2 and earlier were found to contain a local privilege escalation vulnerability which could allow an authenticated, local administrator to run specific executables on the Nessus Agent host. Tenable has included a fix for this issue in Nessus 10.0.0. The installation files can be obtained from the Tenable Downloads Portal (https://www.tenable.com/downloads/nessus).	2021-11-03	4.6	CVE-2021-20135 MISC
tendacn -- ac9_firmware	Buffer Overflow vulnerability in Tenda AC9 V1.0 through V15.03.05.19(6318), and AC9 V3.0 V15.03.06.42_multi, allows attackers to execute arbitrary code via the index parameter.	2021-10-29	5.8	CVE-2021-31627 MISC MISC
tendacn -- ac9_firmware	Buffer Overflow vulnerability in Tenda AC9 V1.0 through V15.03.05.19(6318), and AC9 V3.0 V15.03.06.42_multi, allows attackers to execute arbitrary code via the urls parameter.	2021-10-29	5.8	CVE-2021-31624 MISC MISC
text2pdf_project -- text2pdf	An issue was discovered in function StartPage in text2pdf.c in pdfcorner text2pdf 1.1, allows attackers to cause denial of service or possibly other undisclosed impacts.	2021-11-03	6.8	CVE-2020-23680 MISC MISC
tipsandtricks-hq -- far_future_expiry_header	The Far Future Expiry Header WordPress plugin before 1.5 does not have CSRF check when saving its settings, which could allow attackers to make a logged in admin change them via a CSRF attack.	2021-11-01	4.3	CVE-2021-24799 MISC
vaadin -- vaadin	Missing output sanitization in test sources in org.webjars.bowergithub.vaadin:vaadin-menu-bar versions 1.0.0 through 1.2.0 (Vaadin 14.0.0 through 14.4.4) allows remote attackers to execute malicious JavaScript in browser by opening crafted URL	2021-11-02	4.3	CVE-2021-33611 CONFIRM CONFIRM
validator_project -- validator	validator.js is vulnerable to Inefficient Regular Expression Complexity	2021-11-02	5	CVE-2021-3765 CONFIRM MISC
vmware -- installbuilder	Under certain circumstances, when manipulating the Windows registry, InstallBuilder uses the reg.exe system command. The full path to the command is not enforced, which results in a search in the search path until a binary can be identified. This makes the installer/uninstaller vulnerable to Path Interception by Search Order Hijacking, potentially allowing an attacker to plant a malicious reg.exe command so it takes precedence over the system command. The vulnerability only affects Windows installers.	2021-10-29	4.4	CVE-2021-22037 MISC
vmware -- installbuilder	On Windows, the uninstaller binary copies itself to a fixed temporary location, which is then executed (the originally called uninstaller exits, so it does not block the installation directory). This temporary location is not randomized and does not restrict access to Administrators only so a potential attacker could plant a binary to replace the copied binary right before it gets called, thus gaining Administrator privileges (if the original uninstaller was executed as Administrator). The vulnerability only affects Windows installers.	2021-10-29	6.5	CVE-2021-22038 MISC
wdja -- wdja_cms	Cross Site Scripting (XSS) vulnerability in shadoweb wdja v1.5.1, allows attackers to execute arbitrary code and gain escalated privileges, via the backurl parameter to /php/passport/index.php.	2021-11-03	6.8	CVE-2020-20982 MISC
wordplus -- bp_better_messages	The BP Better Messages WordPress plugin before 1.9.9.41 sanitise (with sanitize_text_field) but does not escape the 'subject' parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting issue	2021-11-01	4.3	CVE-2021-24808 MISC CONFIRM
wordplus -- bp_better_messages	The BP Better Messages WordPress plugin before 1.9.9.41 does not check for CSRF in multiple of its AJAX actions: bp_better_messages_leave_chat, bp_better_messages_join_chat, bp_messages_leave_thread, bp_messages_mute_thread, bp_messages_unmute_thread, bp_better_messages_add_user_to_thread, bp_better_messages_exclude_user_from_thread. This could allow attackers to make logged in users do unwanted actions	2021-11-01	6.8	CVE-2021-24809 CONFIRM MISC
wp-pro-quiz_project -- wp-pro-quiz	The WP-Pro-Quiz WordPress plugin through 0.37 does not have CSRF check in place when deleting a quiz, which could allow an attacker to make a logged in admin delete arbitrary quiz on the blog	2021-11-01	4.3	CVE-2020-36504 MISC MISC
wp-stats_project -- wp-stats	The WP-Stats WordPress plugin before 2.52 does not have CSRF check when saving its settings, and did not escape some of them when outputting them, allowing attacker to make logged in high privilege users change them and set Cross-Site Scripting payloads	2021-11-01	4.3	CVE-2015-10001 MISC MISC
wp_attachment_export_project -- wp_attachment_export	The WP Attachment Export WordPress plugin before 0.2.4 does not have proper access controls, allowing unauthenticated users to download the XML data that holds all the details of attachments/posts on a Wordpress	2021-11-01	5	CVE-2015-20067 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wpplugin -- accept_donations_with_paypal	The Accept Donations with PayPal WordPress plugin before 1.3.1 offers a function to create donation buttons, which internally are posts. The process to create a new button is lacking a CSRF check. An attacker could use this to make an authenticated admin create a new button. Furthermore, one of the Button field is not escaped before being output in an attribute when editing a Button, leading to a Stored Cross-Site Scripting issue as well.	2021-11-01	4.3	CVE-2021-24570 MISC CONFIRM
wpplugin -- accept_donations_with_paypal	The Accept Donations with PayPal WordPress plugin before 1.3.1 provides a function to create donation buttons which are internally stored as posts. The deletion of a button is not CSRF protected and there is no control to check if the deleted post was a button post. As a result, an attacker could make logged in admins delete arbitrary posts	2021-11-01	4.3	CVE-2021-24572 MISC
youyou -- turbocrm	SQL Injection vulnerability exists in all versions of Yonyou TurboCRM.via the orgcode parameter in changepswd.php. Attackers can use the vulnerabilities to obtain sensitive database information.	2021-10-29	5	CVE-2021-41746 MISC MISC
zibbs_project -- zibbs	Cross site scripting (XSS) vulnerability in application/controllers/AdminController.php in xujinliang zibbs 1.0, allows attackers to execute arbitrary code via the bbsmeta parameter.	2021-11-02	6.8	CVE-2020-23719 MISC
zibbs_project -- zibbs	Cross site scripting (XSS) vulnerability in xujinliang zibbs 1.0, allows attackers to execute arbitrary code via the route parameter to index.php.	2021-11-02	6.8	CVE-2020-23718 MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
artica -- pandora_fms	Pandora FMS through 755 allows XSS via a new Event Filter with a crafted name.	2021-11-03	3.5	CVE-2021-36698 MISC MISC MISC
bracketspace -- notification	The Notification WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/src/classes/Utils/Settings.php file which made it possible for attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 7.2.4. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	2021-11-01	2.1	CVE-2021-39340 MISC MISC MISC
cisco -- evolved_programmable_network_manager	A vulnerability in the web-based management interface of Cisco Prime Infrastructure (PI) and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2021-11-04	3.5	CVE-2021-34784 CISCO
cisco -- prime_access_registrar	A vulnerability in the web-based management interface of Cisco Prime Access Registrar could allow an authenticated, remote attacker to perform a stored cross-site scripting attack on an affected system. This vulnerability exists because the web-based management interface does not sufficiently validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need valid administrative credentials. Cisco expects to release software updates that address this vulnerability.	2021-11-04	3.5	CVE-2021-34731 CISCO
connections-pro -- connections_business_directory	The Connections Business Directory WordPress plugin before 10.4.3 does not escape the Address settings when creating an Entry, which could allow high privilege users to perform Cross-Site Scripting when the unfiltered_html capability is disallowed.	2021-11-01	3.5	CVE-2021-24794 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
content_text_slider_on_post_project -- content_text_slider_on_post	The Content text slider on post WordPress plugin before 6.9 does not sanitise and escape the Title and Message/Content settings, which could lead to Cross-Site Scripting issues	2021-11-01	3.5	CVE-2015-20019 MISC CONFIRM MISC
dazzlersoftware -- coming_soon\,_under_construction_amp;_maintenance_mode_by_dazzler	The Coming Soon, Under Construction & Maintenance Mode By Dazzler WordPress plugin before 1.6.7 does not sanitise or escape its description setting when outputting it in the frontend when the Coming Soon mode is enabled, even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue	2021-11-01	2.1	CVE-2021-24539 MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter name of the API schedule, which may allow an attacker to remotely execute code.	2021-11-03	3.5	CVE-2021-38428 MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter deviceName of the API modbusWriter-Reader, which may allow an attacker to remotely execute code.	2021-11-03	3.5	CVE-2021-38411 MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter supplier of the API maintenance, which may allow an attacker to remotely execute code.	2021-11-03	3.5	CVE-2021-38403 MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter comment of the API events, which may allow an attacker to remotely execute code.	2021-11-03	3.5	CVE-2021-38488 MISC
deltaww -- dialink	Delta Electronics DIALink versions 1.2.4.0 and prior is vulnerable to cross-site scripting because an authenticated attacker can inject arbitrary JavaScript code into the parameter name of the API devices, which may allow an attacker to remotely execute code.	2021-11-03	3.5	CVE-2021-38407 MISC
dynpg -- dynpg	Cross Site Scripting (XSS) vulnerability in DynPG 4.9.1, allows authenticated attackers to execute arbitrary code via the groupname.	2021-11-02	3.5	CVE-2020-27406 MISC MISC
e-dynamics -- events_made_easy	The Events Made Easy WordPress plugin before 2.2.24 does not sanitise and escape Custom Field Names, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2021-11-01	3.5	CVE-2021-24813 CONFIRM MISC
etruel -- wpematico_rss_feed_fetcher	The WPeMatico RSS Feed Fetcher WordPress plugin before 2.6.12 does not escape the Feed URL added to a campaign before outputting it in an attribute, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	2021-11-01	3.5	CVE-2021-24793 MISC
flat_preloader_project -- flat_preloader	The Flat Preloader WordPress plugin before 1.5.5 does not escape some of its settings when outputting them in attribute in the frontend, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed	2021-11-01	3.5	CVE-2021-24789 MISC
fortinet -- fortianalyzer	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiAnalyzer version 6.0.6 and below, version 6.4.4 allows attacker to execute unauthorized code or commands via specifically crafted requests to the web GUI.	2021-11-02	3.5	CVE-2020-12814 CONFIRM
fortinet -- forticlient	An improper control of generation of code vulnerability [CWE-94] in FortiClientMacOS versions 7.0.0 and below and 6.4.5 and below may allow an authenticated attacker to hijack the MacOS camera without the user permission via the malicious dylib file.	2021-11-02	3.5	CVE-2021-42754 CONFIRM
fortinet -- forticlient_enterprise_management_server	An improper neutralization of input vulnerability [CWE-79] in FortiClientEMS versions 6.4.1 and below and 6.2.9 and below may allow a remote authenticated attacker to inject malicious script/tags via the name parameter of various sections of the server.	2021-11-02	3.5	CVE-2020-15940 CONFIRM
fortinet -- fortimanager	An exposure of sensitive information to an unauthorized actor [CWE-200] vulnerability in FortiManager 7.0.1 and below, 6.4.6 and below, 6.2.x, 6.0.x, 5.6.0 may allow a FortiGate user to see scripts from other ADOMS.	2021-11-03	2.1	CVE-2021-36192 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortiportal	A concurrent execution using shared resource with improper Synchronization vulnerability ('Race Condition') in the customer database interface of FortiPortal before 6.0.6 may allow an authenticated, low-privilege user to bring the underlying database data into an inconsistent state via specific coordination of web requests.	2021-11-02	3.5	CVE-2021-36181 CONFIRM
fortinet -- fortisiem	A unprotected storage of credentials in Fortinet FortiSIEM Windows Agent version 4.1.4 and below allows an authenticated user to disclosure agent password due to plaintext credential storage in log files	2021-11-02	2.1	CVE-2021-41023 CONFIRM
gitlab -- gitlab	A stored Cross-Site Scripting vulnerability in the DataDog integration in GitLab CE/EE version 13.7 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf	2021-11-05	3.5	CVE-2021-22260 CONFIRM MISC MISC
hp -- futuresmart_3	Certain HP LaserJet, HP LaserJet Managed, HP PageWide, and HP PageWide Managed printers may be vulnerable to potential information disclosure.	2021-11-03	2.1	CVE-2021-39237 MISC
hp -- futuresmart_4	Certain HP Enterprise LaserJet and PageWide MFPs may be vulnerable to stored cross site scripting (XSS).	2021-10-29	3.5	CVE-2021-3662 MISC
hp -- officejet_7110_firmware	A potential security vulnerability has been identified for the HP OfficeJet 7110 Wide Format ePrinter that enables Cross-Site Scripting (XSS).	2021-10-29	3.5	CVE-2021-3441 MISC
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2021-11-02	3.5	CVE-2021-29771 CONFIRM XF
jupyter -- nbdime	nbdime provides tools for diffing and merging of Jupyter Notebooks. In affected versions a stored cross-site scripting (XSS) issue exists within the Jupyter-owned nbdime project. It appears that when reading the file name and path from disk, the extension does not sanitize the string it constructs before returning it to be displayed. The diffNotebookCheckpoint function within nbdime causes this issue. When attempting to display the name of the local notebook (diffNotebookCheckpoint), nbdime appears to simply append .ipynb to the name of the input file. The NbdimeWidget is then created, and the base string is passed through to the request API function. From there, the frontend simply renders the HTML tag and anything along with it. Users are advised to patch to the most recent version of the affected product.	2021-11-03	3.5	CVE-2021-41134 MISC CONFIRM
libjxl_project -- libjxl	Invalid JPEG XL images using libjxl can cause an out of bounds access on a std::vector<std::vector<T>> when rendering splines. The OOB read access can either lead to a segfault, or rendering splines based on other process memory. It is recommended to upgrade past 0.6.0 or patch with https://github.com/libjxl/libjxl/pull/757	2021-11-01	3.6	CVE-2021-22563 CONFIRM CONFIRM
libjxl_project -- libjxl	For certain valid JPEG XL images with a size slightly larger than an integer number of groups (256x256 pixels) when processing the groups out of order the decoder can perform an out of bounds copy of image pixels from an image buffer in the heap to another. This copy can occur when processing the right or bottom edges of the image, but only when groups are processed in certain order. Groups can be processed out of order in multi-threaded decoding environments with heavy thread load but also with images that contain the groups in an arbitrary order in the file. It is recommended to upgrade past 0.6.0 or patch with https://github.com/libjxl/libjxl/pull/775	2021-11-01	2.1	CVE-2021-22564 CONFIRM CONFIRM
mahara -- mahara	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, adjusting the path component for the page help file allows attackers to bypass the intended access control for HTML files via directory traversal. It replaces the - character with the / character.	2021-11-02	2.1	CVE-2021-43264 MISC MISC
mahara -- mahara	In Mahara before 20.04.5, 20.10.3, 21.04.2, and 21.10.0, certain tag syntax could be used for XSS, such as via a SCRIPT element.	2021-11-02	3.5	CVE-2021-43265 MISC MISC
mcafee -- data_loss_prevention_endpoint	Cross site scripting (XSS) vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.7.100 allows a remote attacker to highjack an active DLP ePO administrator session by convincing the logged in administrator to click on a carefully crafted link in the case management part of the DLP ePO extension.	2021-11-01	3.5	CVE-2021-31848 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
motopress -- restaurant_menu	The Restaurant Menu by MotoPress WordPress plugin through 2.4.0 does not properly sanitize or escape inputs when creating new menu items, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	2021-11-01	3.5	CVE-2021-24722 MISC
netapp -- ontap_system_manager	System Manager 9.x versions 9.7 and higher prior to 9.7P16, 9.8P7 and 9.9.1P2 are susceptible to a vulnerability which could allow a local attacker to discover plaintext iSCSI CHAP credentials.	2021-11-01	1.7	CVE-2021-27004 MISC
nvidia -- virtual_gpu	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager kernel driver, where a vGPU can cause resource starvation among other vGPUs hosted on the same GPU, which may lead to denial of service.	2021-10-29	2.1	CVE-2021-1121 CONFIRM
nvidia -- virtual_gpu	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can dereference a NULL pointer, which may lead to denial of service.	2021-10-29	2.1	CVE-2021-1122 CONFIRM
nvidia -- virtual_gpu	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can deadlock, which may lead to denial of service.	2021-10-29	2.1	CVE-2021-1123 CONFIRM
nvidia -- virtual_gpu	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where it can double-free a pointer, which may lead to denial of service. This flaw may result in a write-what-where condition, allowing an attacker to execute arbitrary code impacting integrity and availability.	2021-10-29	3.6	CVE-2021-1119 CONFIRM
online_event_booking_and_reservation_system_project -- online_event_booking_and_reservation_system	A Stored Cross Site Scripting (XSS) vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP/MySQL via the Holiday reason parameter. An attacker can leverage this vulnerability in order to run javascript commands on the web server surfers behalf, which can lead to cookie stealing and more.	2021-11-05	3.5	CVE-2021-42662 MISC MISC MISC
snowsoftware -- snow_inventory_agent	A vulnerability in Snow Snow Agent for Windows allows a non-admin user to cause arbitrary deletion of files. This issue affects: Snow Snow Agent for Windows version 5.0.0 to 6.7.1 on Windows.	2021-11-03	3.6	CVE-2021-41562 MISC
sonaar -- mp3_audio_player_for_music\,_radio_&amp;_podcast	The MP3 Audio Player for Music, Radio & Podcast by Sonaar WordPress plugin before 2.4.2 does not properly sanitize or escape data in some of its Playlist settings, allowing high privilege users to perform Cross-Site Scripting attacks	2021-11-01	3.5	CVE-2021-24624 MISC
supsystic -- easy_google_maps	The Google Maps Easy WordPress plugin is vulnerable to Stored Cross-Site Scripting due to insufficient input validation and sanitization via several parameters found in the ~/modules/marker_groups/views/tpl/mgrEditMarkerGroup.php file which allowed attackers with administrative user access to inject arbitrary web scripts, in versions up to and including 1.9.33. This affects multi-site installations where unfiltered_html is disabled for administrators, and sites where unfiltered_html is disabled.	2021-11-01	2.1	CVE-2021-39346 MISC MISC MISC
webnus -- modern_events_calendar_lite	The Modern Events Calendar Lite WordPress plugin before 5.22.3 does not properly sanitize or escape values set by users with access to adjust settings withing wp-admin.	2021-11-01	3.5	CVE-2021-24716 MISC
wp_sitemap_page_project -- wp_sitemap_page	The WP Sitemap Page WordPress plugin before 1.7.0 does not properly sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	2021-11-01	3.5	CVE-2021-24715 MISC
wpdownloadmanager -- wordpress_download_manager	The WordPress Download Manager WordPress plugin before 3.2.16 does not escape some of the Download settings when outputting them, allowing high privilege users to perform XSS attacks even when the unfiltered_html capability is disallowed	2021-11-01	3.5	CVE-2021-24773 MISC
wpkube -- cool_tag_cloud	The Cool Tag Cloud WordPress plugin before 2.26 does not escape the style attribute of the cool_tag_cloud shortcode, which could allow users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks.	2021-11-01	3.5	CVE-2021-24682 MISC
wpreactions -- wp_reactions_lite	The WP Reactions Lite WordPress plugin before 1.3.6 does not properly sanitize inputs within wp-admin pages, allowing users with sufficient access to inject XSS payloads within /wp-admin/ pages.	2021-11-01	3.5	CVE-2021-24723 MISC
xenforo -- xenforo	In XenForo through 2.2.7, a threat actor with access to the admin panel can create a new Advertisement via the Advertising function, and save an XSS payload in the body of the HTML document. This payload will execute globally on the client side.	2021-11-03	3.5	CVE-2021-43032 MISC MISC

Back to top

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
android -- samsung	Improper privilege management vulnerability in API Key used in SmartThings prior to 1.7.73.22 allows an attacker to abuse the API key without limitation.	2021-11-05	not yet calculated	CVE-2021-25508 MISC
android -- samsung	An improper access control vulnerability in SCloudBnRReceiver in SecTelephonyProvider prior to SMR Nov-2021 Release 1 allows untrusted application to call some protected providers.	2021-11-05	not yet calculated	CVE-2021-25501 MISC
android -- samsung	AVideo/YouPHPTube 10.0 and prior is affected by Insecure file write. An administrator privileged user is able to write files on filesystem using flag and code variables in file save.php.	2021-11-01	not yet calculated	CVE-2021-25877 MISC MISC MISC
android -- samsung	A vulnerability of storing sensitive information insecurely in Property Settings prior to SMR Nov-2021 Release 1 allows attackers to read ESN value without priviledge.	2021-11-05	not yet calculated	CVE-2021-25502 MISC
android -- samsung	Intent redirection vulnerability in Group Sharing prior to 10.8.03.2 allows attacker to access contact information.	2021-11-05	not yet calculated	CVE-2021-25504 MISC
android -- samsung	AVideo/YouPHPTube 10.0 and prior has multiple reflected Cross Script Scripting vulnerabilities via the u parameter which allows a remote attacker to steal administrators' session cookies or perform actions as an administrator.	2021-11-01	not yet calculated	CVE-2021-25876 MISC MISC MISC
android -- samsung	A cross-site scripting (XSS) vulnerability in Power Admin PA Server Monitor 8.2.1.1 allows remote attackers to inject arbitrary web script or HTML via Console.exe.	2021-11-05	not yet calculated	CVE-2021-26844 MISC MISC
android -- samsung	AVideo/YouPHPTube 10.0 and prior is affected by multiple reflected Cross Script Scripting vulnerabilities via the videoName parameter which allows a remote attacker to steal administrators' session cookies or perform actions as an administrator.	2021-11-01	not yet calculated	CVE-2021-25878 MISC MISC MISC
android -- samsung	A missing input validation in HDCP LDFW prior to SMR Nov-2021 Release 1 allows attackers to overwrite TZASC allowing TEE compromise.	2021-11-05	not yet calculated	CVE-2021-25500 MISC
android -- samsung	Improper input validation vulnerability in HDCP prior to SMR Nov-2021 Release 1 allows attackers to arbitrary code execution.	2021-11-05	not yet calculated	CVE-2021-25503 MISC
android -- samsung	Improper authentication in Samsung Pass prior to 3.0.02.4 allows to use app without authentication when lockscreen is unlocked.	2021-11-05	not yet calculated	CVE-2021-25505 MISC
android -- samsung	Non-existent provider in Samsung Health prior to 6.19.1.0001 allows attacker to access it via malicious content provider or lead to denial of service.	2021-11-05	not yet calculated	CVE-2021-25506 MISC
android -- samsung	Improper authorization vulnerability in Samsung Flow mobile application prior to 4.8.03.5 allows Samsung Flow PC application connected with user device to access part of notification data in Secure Folder without authorization.	2021-11-05	not yet calculated	CVE-2021-25507 MISC
android -- samsung	A missing input validation in Samsung Flow Windows application prior to Version 4.8.5.0 allows attackers to overwrite abtraty file in the Windows known folders.	2021-11-05	not yet calculated	CVE-2021-25509 MISC
android -- samsung	AVideo/YouPHPTube AVideo/YouPHPTube 10.0 and prior is affected by a SQL Injection SQL injection in the catName parameter which allows a remote unauthenticated attacker to retrieve databases information such as application passwords hashes.	2021-11-01	not yet calculated	CVE-2021-25874 MISC MISC MISC
android -- samsung	AVideo/YouPHPTube AVideo/YouPHPTube 10.0 and prior has multiple reflected Cross Script Scripting vulnerabilities via the searchPhrase parameter which allows a remote attacker to steal administrators' session cookies or perform actions as an administrator.	2021-11-01	not yet calculated	CVE-2021-25875 MISC MISC MISC
ayacms -- ayacms	Cross site request forgery (CSRF) vulnerability in AyaCMS 3.1.2 allows attackers to change an administrators password or other unspecified impacts.	2021-11-02	not yet calculated	CVE-2020-23686 MISC
azeotech -- daqfactory	An attacker could prepare a specially crafted project file that, if opened, would attempt to connect to the cloud and trigger a man in the middle (MiTM) attack. This could allow an attacker to obtain credentials and take over the user’s cloud account.	2021-11-05	not yet calculated	CVE-2021-42701 MISC
azeotech -- daqfactory	The affected application uses specific functions that could be abused through a crafted project file, which could lead to code execution, system reboot, and system shutdown.	2021-11-05	not yet calculated	CVE-2021-42543 MISC
azeotech -- daqfactory	Project files are stored memory objects in the form of binary serialized data that can later be read and deserialized again to instantiate the original objects in memory. Malicious manipulation of these files may allow an attacker to corrupt memory.	2021-11-05	not yet calculated	CVE-2021-42698 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
azeotech -- daqfactory	The affected product is vulnerable to cookie information being transmitted as cleartext over HTTP. An attacker can capture network traffic, obtain the user's cookie and take over the account.	2021-11-05	not yet calculated	CVE-2021-42699 MISC
bluez -- bluez	An issue was discovered in gatt-database.c in BlueZ 5.61. A use-after-free can occur when a client disconnects during D-Bus processing of a WriteValue call.	2021-11-04	not yet calculated	CVE-2021-43400 MISC
bookstack -- bookstack	bookstack is vulnerable to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2021-11-05	not yet calculated	CVE-2021-3916 CONFIRM MISC
cisco -- asyncos	A vulnerability in the email scanning algorithm of Cisco AsyncOS software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to perform a denial of service (DoS) attack against an affected device. This vulnerability is due to insufficient input validation of incoming emails. An attacker could exploit this vulnerability by sending a crafted email through Cisco ESA. A successful exploit could allow the attacker to exhaust all the available CPU resources on an affected device for an extended period of time, preventing other emails from being processed and resulting in a DoS condition.	2021-11-04	not yet calculated	CVE-2021-34741 CISCO
cisco -- multiple_products	A vulnerability in the web-based management interface of Cisco Small Business 200 Series Smart Switches, Cisco Small Business 300 Series Managed Switches, and Cisco Small Business 500 Series Stackable Managed Switches could allow an unauthenticated, remote attacker to render the web-based management interface unusable, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to cause a permanent invalid redirect for requests sent to the web-based management interface of the device, resulting in a DoS condition.	2021-11-04	not yet calculated	CVE-2021-40127 CISCO
cisco -- policy_suite	A vulnerability in the key-based SSH authentication mechanism of Cisco Policy Suite could allow an unauthenticated, remote attacker to log in to an affected system as the root user. This vulnerability is due to the re-use of static SSH keys across installations. An attacker could exploit this vulnerability by extracting a key from a system under their control. A successful exploit could allow the attacker to log in to an affected system as the root user.	2021-11-04	not yet calculated	CVE-2021-40119 CISCO
cisco -- small_business_series_switches	A vulnerability in the web-based management interface of multiple Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to replay valid user session credentials and gain unauthorized access to the web-based management interface of an affected device. This vulnerability is due to insufficient expiration of session credentials. An attacker could exploit this vulnerability by conducting a man-in-the-middle attack against an affected device to intercept valid session credentials and then replaying the intercepted credentials toward the same device at a later time. A successful exploit could allow the attacker to access the web-based management interface with administrator privileges.	2021-11-04	not yet calculated	CVE-2021-34739 CISCO
couchbase -- server	Couchbase Server before 6.6.3 and 7.x before 7.0.2 stores Sensitive Information in Cleartext. The issue occurs when the cluster manager forwards a HTTP request from the pluggable UI (query workbench etc) to the specific service. In the backtrace, the Basic Auth Header included in the HTTP request, has the "@" user credentials of the node processing the UI request.	2021-11-02	not yet calculated	CVE-2021-42763 MISC MISC
couchbase -- server	metakv in Couchbase Server 7.0.0 uses Cleartext for Storage of Sensitive Information. Remote Cluster XDCR credentials can get leaked in debug logs. Config key tombstone purging was added in Couchbase Server 7.0.0. This issue happens when a config key, which is being logged, has a tombstone purger time-stamp attached to it.	2021-11-02	not yet calculated	CVE-2021-37842 MISC MISC
crypto++ -- crypto++	Crypto++ (aka Cryptopp) 8.6.0 and earlier contains a timing leakage in MakePublicKey(). There is a clear correlation between execution time and private key length, which may cause disclosure of the length information of the private key. This might allow attackers to conduct timing attacks.	2021-11-04	not yet calculated	CVE-2021-43398 MISC MISC
d-link -- dir-823g_devices	A command injection vulnerability was discovered in the HNAP1 protocol in D-Link DIR-823G devices with firmware V1.0.2B05. An attacker is able to execute arbitrary web scripts via shell metacharacters in the PrivateLogin field to Login.	2021-11-04	not yet calculated	CVE-2020-25368 MISC MISC MISC
fusionpbx -- fusionpbx	An issue was discovered in FusionPBX before 4.5.30. The fax_post_size may have risky characters (it is not constrained to preset values).	2021-11-05	not yet calculated	CVE-2021-43406 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fusionpbx -- fusionpbx	An issue was discovered in FusionPBX before 4.5.30. The FAX file name may have risky characters.	2021-11-05	not yet calculated	CVE-2021-43404 MISC
fusionpbx -- fusionpbx	An issue was discovered in FusionPBX before 4.5.30. The fax_extension may have risky characters (it is not constrained to be numeric).	2021-11-05	not yet calculated	CVE-2021-43405 MISC
gitlab -- ce/ee	In all versions of GitLab CE/EE since version 10.6, a project export leaks the external webhook token value which may allow access to the project which it was exported from.	2021-11-05	not yet calculated	CVE-2021-39898 MISC CONFIRM MISC
gitlab -- ce/ee	In all versions of GitLab CE/EE since version 13.0, a privileged user, through an API call, can change the visibility level of a group or a project to a restricted option even after the instance administrator sets that visibility option as restricted in settings.	2021-11-04	not yet calculated	CVE-2021-39903 MISC CONFIRM MISC
gitlab -- ce/ee	Improper validation of ipynb files in GitLab CE/EE version 13.5 and above allows an attacker to execute arbitrary JavaScript code on the victim's behalf.	2021-11-05	not yet calculated	CVE-2021-39906 MISC CONFIRM MISC
gitlab -- ce/ee	A potential DOS vulnerability was discovered in GitLab CE/EE starting with version 13.7. The stripping of EXIF data from certain images resulted in high CPU usage.	2021-11-05	not yet calculated	CVE-2021-39907 MISC CONFIRM MISC
gitlab -- ce/ee	An improper access control flaw in GitLab CE/EE since version 13.9 exposes private email address of Issue and Merge Requests assignee to Webhook data consumers	2021-11-05	not yet calculated	CVE-2021-39911 MISC CONFIRM
gitlab -- ce/ee	A regular expression denial of service issue in GitLab versions 8.13 to 14.2.5, 14.3.0 to 14.3.3 and 14.4.0 could cause excessive usage of resources when a specially crafted username was used when provisioning a new user	2021-11-04	not yet calculated	CVE-2021-39914 MISC CONFIRM
gitlab -- ce/ee	In all versions of GitLab CE/EE since version 8.0, an attacker can set the pipeline schedules to be active in a project export so when an unsuspecting owner imports that project, pipelines are active by default on that project. Under specialized conditions, this may lead to information disclosure if the project is imported from an untrusted source.	2021-11-05	not yet calculated	CVE-2021-39895 MISC CONFIRM MISC
gitlab -- ce/ee	Improper access control in GitLab CE/EE version 10.5 and above allowed subgroup members with inherited access to a project from a parent group to still have access even after the subgroup is transferred	2021-11-05	not yet calculated	CVE-2021-39897 MISC CONFIRM MISC
gitlab -- ce/ee	In all versions of GitLab CE/EE since version 11.10, an admin of a group can see the SCIM token of that group by visiting a specific endpoint.	2021-11-05	not yet calculated	CVE-2021-39901 MISC CONFIRM MISC
gitlab -- ce/ee	An Improper Access Control vulnerability in the GraphQL API in GitLab CE/EE since version 13.1 allows a Merge Request creator to resolve discussions and apply suggestions after a project owner has locked the Merge Request	2021-11-05	not yet calculated	CVE-2021-39904 CONFIRM MISC MISC
gitlab -- ce/ee	A potential DoS vulnerability was discovered in GitLab CE/EE starting with version 13.7. Using a malformed TIFF images was possible to trigger memory exhaustion.	2021-11-05	not yet calculated	CVE-2021-39912 CONFIRM MISC MISC
gitlab -- ce/ee	Accidental logging of system root password in the migration log in all versions of GitLab CE/EE allows an attacker with local file system access to obtain system root-level privileges	2021-11-05	not yet calculated	CVE-2021-39913 CONFIRM MISC
gitlab -- ce/ee	Incorrect Authorization in GitLab CE/EE 13.4 or above allows a user with guest membership in a project to modify the severity of an incident.	2021-11-04	not yet calculated	CVE-2021-39902 MISC MISC CONFIRM
gitlab -- ce/ee	An information disclosure vulnerability in the GitLab CE/EE API since version 8.9.6 allows a user to see basic information on private groups that a public project has been shared with	2021-11-05	not yet calculated	CVE-2021-39905 MISC CONFIRM MISC
gitlab -- ee/ee	Lack of email address ownership verification in the CODEOWNERS feature in all versions of GitLab EE since version 11.3 allows an attacker to bypass CODEOWNERS Merge Request approval requirement under rare circumstances	2021-11-05	not yet calculated	CVE-2021-39909 MISC MISC CONFIRM
gnu_library -- glibc	In iconvdata/iso-2022-jp-3.c in the GNU C Library (aka glibc) 2.34, remote attackers can force iconv() to emit a spurious ' ' character via crafted ISO-2022-JP-3 data that is accompanied by an internal state reset. This may affect data integrity in certain iconv() use cases.	2021-11-04	not yet calculated	CVE-2021-43396 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
graphiql -- graphiql	GraphiQL is the reference implementation of this monorepo, GraphQL IDE, an official project under the GraphQL Foundation. All versions of graphiql older than graphiql@1.4.7 are vulnerable to compromised HTTP schema introspection responses or schema prop values with malicious GraphQL type names, exposing a dynamic XSS attack surface that can allow code injection on operation autocomplete. In order for the attack to take place, the user must load a vulnerable schema in graphiql. There are a number of ways that can occur. By default, the schema URL is not attacker-controllable in graphiql or in its suggested implementations or examples, leaving only very complex attack vectors. If a custom implementation of graphiql's fetcher allows the schema URL to be set dynamically, such as a URL query parameter like ?endpoint= in graphql-playground, or a database provided value, then this custom graphiql implementation is vulnerable to phishing attacks, and thus much more readily available, low or no privelege level xss attacks. The URLs could look like any generic looking graphql schema URL. It should be noted that desktop clients such as Altair, Insomnia, Postwoman, do not appear to be impacted by this. This vulnerability does not impact codemirror-graphql, monaco-graphql or other dependents, as it exists in onHasCompletion.ts in graphiql. It does impact all forks of graphiql, and every released version of graphiql.	2021-11-04	not yet calculated	CVE-2021-41248 MISC CONFIRM MISC
graphiql -- graphql_plyground	GraphQL Playground is a GraphQL IDE for development of graphQL focused applications. All versions of graphql-playground-react older than graphql-playground-react@1.7.28 are vulnerable to compromised HTTP schema introspection responses or schema prop values with malicious GraphQL type names, exposing a dynamic XSS attack surface that can allow code injection on operation autocomplete. In order for the attack to take place, the user must load a malicious schema in graphql-playground. There are several ways this can occur, including by specifying the URL to a malicious schema in the endpoint query parameter. If a user clicks on a link to a GraphQL Playground installation that specifies a malicious server, arbitrary JavaScript can run in the user's browser, which can be used to exfiltrate user credentials or other harmful goals. If you are using graphql-playground-react directly in your client app, upgrade to version 1.7.28 or later.	2021-11-04	not yet calculated	CVE-2021-41249 CONFIRM MISC MISC
grav -- grav	grav is vulnerable to Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2021-11-05	not yet calculated	CVE-2021-3924 CONFIRM MISC
hewlett_packard -- pagewide_and_officejet	HP has identified a security vulnerability with the I.R.I.S. OCR (Optical Character Recognition) software available with HP PageWide and OfficeJet printer software installations that could potentially allow unauthorized local code execution.	2021-11-03	not yet calculated	CVE-2020-28416 MISC
ibm -- business_automation_workflo	IBM Business Automation Workflow 18. 19, 20, 21, and IBM Business Process Manager 8.5 and d8.6 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval.	2021-11-05	not yet calculated	CVE-2021-29753 CONFIRM XF
insyde -- insydeh2o	An issue was discovered in Int15MicrocodeSmm in Insyde InsydeH2O before 2021-10-14 on Intel client chipsets. A caller may be able to escalate privileges.	2021-11-03	not yet calculated	CVE-2020-5955 CONFIRM MISC
irfanview -- irfanview	Irfanview v4.53 was discovered to contain an infinity loop via JPEG2000!ShowPlugInSaveOptions_W+0x1ecd8.	2021-11-05	not yet calculated	CVE-2020-23566 MISC
irfanview -- irfanview	Irfanview v4.53 allows attackers to to cause a denial of service (DoS) via a crafted JPEG 2000 file. Related to "Integer Divide By Zero starting at JPEG2000!ShowPlugInSaveOptions_W+0x00000000000082ea"	2021-11-05	not yet calculated	CVE-2020-23567 MISC
irfanview -- irfanview	Irfanview v4.53 allows attackers to execute arbitrary code via a crafted JPEG 2000 file. Related to a "Data from Faulting Address controls Branch Selection starting at JPEG2000!ShowPlugInSaveOptions_W+0x0000000000032850".	2021-11-05	not yet calculated	CVE-2020-23565 MISC
jeedom -- jeedom	In Jeedom through 4.1.19, a bug allows a remote attacker to bypass API access and retrieve users credentials.	2021-11-01	not yet calculated	CVE-2021-42557 MISC MISC
jenkins -- jenkins	FilePath#toURI, FilePath#hasSymlink, FilePath#absolutize, FilePath#isDescendant, and FilePath#get*DiskSpace do not check any permissions in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	2021-11-04	not yet calculated	CVE-2021-21694 CONFIRM
jenkins -- jenkins	When creating temporary files, agent-to-controller access to create those files is only checked after they've been created in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	2021-11-04	not yet calculated	CVE-2021-21693 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
jenkins -- jenkins	FilePath#listFiles lists files outside directories that agents are allowed to access when following symbolic links in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	2021-11-04	not yet calculated	CVE-2021-21695 CONFIRM MLIST
jenkins -- jenkins	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not limit agent read/write access to the libs/ directory inside build directories when using the FilePath APIs, allowing attackers in control of agent processes to replace the code of a trusted library with a modified variant. This results in unsandboxed code execution in the Jenkins controller process.	2021-11-04	not yet calculated	CVE-2021-21696 CONFIRM MLIST
jenkins -- jenkins	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not check agent-to-controller access to create symbolic links when unarchiving a symbolic link in FilePath#untar.	2021-11-04	not yet calculated	CVE-2021-21687 CONFIRM
jenkins -- jenkins	FilePath#renameTo and FilePath#moveAllChildrenTo in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier only check 'read' agent-to-controller access permission on the source path, instead of 'delete'.	2021-11-04	not yet calculated	CVE-2021-21692 CONFIRM
jenkins -- jenkins	Creating symbolic links is possible without the 'symlink' agent-to-controller access control permission in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	2021-11-04	not yet calculated	CVE-2021-21691 CONFIRM
jenkins -- jenkins	Jenkins Subversion Plugin 2.15.0 and earlier does not restrict the name of a file when looking up a subversion key file on the controller from an agent.	2021-11-04	not yet calculated	CVE-2021-21698 CONFIRM MLIST
jenkins -- jenkins	File path filters in the agent-to-controller security subsystem of Jenkins 2.318 and earlier, LTS 2.303.2 and earlier do not canonicalize paths, allowing operations to follow symbolic links to outside allowed directories.	2021-11-04	not yet calculated	CVE-2021-21686 CONFIRM
jenkins -- jenkins	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier does not check agent-to-controller access to create parent directories in FilePath#mkdirs.	2021-11-04	not yet calculated	CVE-2021-21685 CONFIRM MLIST
jenkins -- jenkins	FilePath#unzip and FilePath#untar were not subject to any agent-to-controller access control in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	2021-11-04	not yet calculated	CVE-2021-21689 CONFIRM
jenkins -- jenkins	Jenkins 2.318 and earlier, LTS 2.303.2 and earlier allows any agent to read and write the contents of any build directory stored in Jenkins with very few restrictions.	2021-11-04	not yet calculated	CVE-2021-21697 CONFIRM MLIST
jenkins -- jenkins	Agent processes are able to completely bypass file path filtering by wrapping the file operation in an agent file path in Jenkins 2.318 and earlier, LTS 2.303.2 and earlier.	2021-11-04	not yet calculated	CVE-2021-21690 CONFIRM
jupyterhub -- jupyter_notebooks	JupyterHub is an open source multi-user server for Jupyter notebooks. In affected versions users who have multiple JupyterLab tabs open in the same browser session, may see incomplete logout from the single-user server, as fresh credentials (for the single-user server only, not the Hub) reinstated after logout, if another active JupyterLab session is open while the logout takes place. Upgrade to JupyterHub 1.5. For distributed deployments, it is jupyterhub in the _user_ environment that needs patching. There are no patches necessary in the Hub environment. The only workaround is to make sure that only one JupyterLab tab is open when you log out.	2021-11-04	not yet calculated	CVE-2021-41247 CONFIRM MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.14.15. There is an array-index-out-of-bounds flaw in the detach_capi_ctr function in drivers/isdn/capi/kcapi.c.	2021-11-04	not yet calculated	CVE-2021-43389 MISC MISC MISC MISC CONFIRM MLIST
meross -- smart_wi-fi_2_way_wall_switch	Meross Smart Wi-Fi 2 Way Wall Switch (MSS550X), on its 3.1.3 version and before, creates an open Wi-Fi Access Point without the required security measures in its initial setup. This could allow a remote attacker to obtain the Wi-Fi SSID as well as the password configured by the user from Meross app via Http/JSON plain request.	2021-11-05	not yet calculated	CVE-2021-3774 CONFIRM
miniftpd -- miniftpd	A local buffer overflow vulnerability exists in the latest version of Miniftpd in ftpproto.c through the tmp variable, where a crafted payload can be sent to the affected function.	2021-11-04	not yet calculated	CVE-2021-42624 MISC
mozilla -- firefox	Possible system denial of service in case of arbitrary changing Firefox browser parameters. An attacker could change specific Firefox browser parameters file in a certain way and then reboot the system to make the system unbootable.	2021-11-03	not yet calculated	CVE-2021-35053 MISC
nec -- clusterpro	Buffer overflow vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network.	2021-11-03	not yet calculated	CVE-2021-20703 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nec -- clusterpro	Buffer overflow vulnerability in the Disk Agent CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network.	2021-11-03	not yet calculated	CVE-2021-20701 MISC
nec -- clusterpro	Buffer overflow vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network.	2021-11-03	not yet calculated	CVE-2021-20702 MISC
nec -- clusterpro	Improper input validation vulnerability in the WebManager CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote file upload via network.	2021-11-03	not yet calculated	CVE-2021-20705 MISC
nec -- clusterpro	Buffer overflow vulnerability in the compatible API with previous versions CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network.	2021-11-03	not yet calculated	CVE-2021-20704 MISC
nec -- clusterpro	Improper input validation vulnerability in the Transaction Server CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to read files upload via network..	2021-11-03	not yet calculated	CVE-2021-20707 MISC
nec -- clusterpro	Buffer overflow vulnerability in the Disk Agent CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote code execution via a network.	2021-11-03	not yet calculated	CVE-2021-20700 MISC
nec -- clusterpro	Improper input validation vulnerability in the WebManager CLUSTERPRO X 1.0 for Windows and later, EXPRESSCLUSTER X 1.0 for Windows and later allows attacker to remote file upload via network.	2021-11-03	not yet calculated	CVE-2021-20706 MISC
obsidian -- dataview	Obsidian Dataview through 0.4.12-hotfix1 allows eval injection. The evalInContext function in executes user input, which allows an attacker to craft malicious Markdown files that will execute arbitrary code once opened. NOTE: 0.4.13 provides a mitigation for some use cases.	2021-11-04	not yet calculated	CVE-2021-42057 MISC
owasp -- modsecurity_core_rule	OWASP ModSecurity Core Rule Set 3.1.x before 3.1.2, 3.2.x before 3.2.1, and 3.3.x before 3.3.2 is affected by a Request Body Bypass via a trailing pathname.	2021-11-05	not yet calculated	CVE-2021-35368 CONFIRM MISC CONFIRM MISC
phpgurukul -- hospital_management_system	Multiple Cross Site Scripting (XSS) vulnerabilities exist in PHPGurukul Hospital Management System 4.0 via the (1) searchdata parameter in (a) doctor/search.php and (b) admin/patient-search.php, and the (2) fromdate and (3) todate parameters in admin/betweendates-detailsreports.php.	2021-11-05	not yet calculated	CVE-2021-39411 MISC
phpgurukul -- shopping	Multiple Cross Site Scripting (XSS) vulnerabilities exists in PHPGurukul Shopping v3.1 via the (1) callback parameter in (a) server_side/scripts/id_jsonp.php, (b) server_side/scripts/jsonp.php, and (c) scripts/objects_jsonp.php, the (2) value parameter in examples_support/editable_ajax.php, and the (3) PHP_SELF parameter in captcha/index.php.	2021-11-05	not yet calculated	CVE-2021-39412 MISC
pomerium -- pomerium	Pomerium is an open source identity-aware access proxy. In affected versions changes to the OIDC claims of a user after initial login are not reflected in policy evaluation when using \`allowed_idp_claims\` as part of policy. If using \`allowed_idp_claims\` and a user's claims are changed, Pomerium can make incorrect authorization decisions. This issue has been resolved in v0.15.6. For users unable to upgrade clear data on \`databroker\` service by clearing redis or restarting the in-memory databroker to force claims to be updated.	2021-11-05	not yet calculated	CVE-2021-41230 CONFIRM MISC
pybbcms -- topicmapper	A SQL injection vulnerability in TopicMapper.xml of PybbsCMS v5.2.1 allows attackers to access sensitive database information.	2021-11-01	not yet calculated	CVE-2020-28702 MISC
python -- discord	Python discord bot is the community bot for the Python Discord community. In affected versions when a non-blacklisted URL and an otherwise triggering filter token is included in the same message the token filter does not trigger. This means that by including any non-blacklisted URL moderation filters can be bypassed. This issue has been resolved in commit 67390298852513d13e0213870e50fb3cff1424e0	2021-11-05	not yet calculated	CVE-2021-41250 MISC CONFIRM
realtek -- rtsupx	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve unauthorized access to USB device privileged IN and OUT instructions (leading to Escalation of Privileges, Denial of Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device.	2021-11-02	not yet calculated	CVE-2021-36923 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
realtek -- rtsupx	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve a pool overflow (leading to Escalation of Privileges, Denial of Service, and Code Execution) via a crafted Device IO Control packet to a device.	2021-11-02	not yet calculated	CVE-2021-36924 MISC MISC
realtek -- rtsupx	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve unauthorized access to USB devices (Escalation of Privileges, Denial of Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device.	2021-11-02	not yet calculated	CVE-2021-36922 MISC MISC
realtek -- rtsupx	RtsUpx.sys in Realtek RtsUpx USB Utility Driver for Camera/Hub/Audio through 1.14.0.0 allows local low-privileged users to achieve an arbitrary read or write operation from/to physical memory (leading to Escalation of Privileges, Denial of Service, Code Execution, and Information Disclosure) via a crafted Device IO Control packet to a device.	2021-11-02	not yet calculated	CVE-2021-36925 MISC MISC
sap -- business_technology_Platform	@sap-cloud-sdk/core contains the core functionality of the SAP Cloud SDK as well as the SAP Business Technology Platform abstractions. This affects applications on SAP Business Technology Platform that use the SAP Cloud SDK and enabled caching of destinations. In affected versions and in some cases, when user information was missing, destinations were cached without user information, allowing other users to retrieve the same destination with its permissions. By default, destination caching is disabled. The security for caching has been increased. The changes are released in version 1.52.0. Users unable to upgrade are advised to disable destination caching (it is disabled by default).	2021-11-05	not yet calculated	CVE-2021-41251 MISC CONFIRM MISC
seo -- panel	Multiple Cross Site Scripting (XSS) vulnerabilities exits in SEO Panel v4.8.0 via the (1) to_time parameter in (a) backlinks.php, (b) analytics.php, (c) log.php, (d) overview.php, (e) pagespeed.php, (f) rank.php, (g) review.php, (h) saturationchecker.php, (i) social_media.php, and (j) reports.php; the (2) from_time parameter in (a) backlinks.php, (b) analytics.php, (c) log.php, (d) overview.php, (e) pagespeed.php, (f) rank.php, (g) review.php, (h) saturationchecker.php, (i) social_media.php, (j) webmaster-tools.php, and (k) reports.php; the (3) order_col parameter in (a) analytics.php, (b) review.php, (c) social_media.php, and (d) webmaster-tools.php; and the (4) pageno parameter in (a) alerts.php, (b) log.php, (c) keywords.php, (d) proxy.php, (e) searchengine.php, and (f) siteauditor.php.	2021-11-05	not yet calculated	CVE-2021-39413 MISC
seo -- remote_clinic	Multiple Cross Site Scripting (XSS) vulnerabilities exists in Remote Clinic v2.0 in (1) patients/register-patient.php via the (a) Contact, (b) Email, (c) Weight, (d) Profession, (e) ref_contact, (f) address, (g) gender, (h) age, and (i) serial parameters; in (2) patients/edit-patient.php via the (a) Contact, (b) Email, (c) Weight, Profession, (d) ref_contact, (e) address, (f) serial, (g) age, and (h) gender parameters; in (3) staff/edit-my-profile.php via the (a) Title, (b) First Name, (c) Last Name, (d) Skype, and (e) Address parameters; and in (4) clinics/settings.php via the (a) portal_name, (b) guardian_short_name, (c) guardian_name, (d) opening_time, (e) closing_time, (f) access_level_5, (g) access_level_4, (h) access_level_ 3, (i) access_level_2, (j) access_level_1, (k) currency, (l) mobile_number, (m) address, (n) patient_contact, (o) patient_address, and (p) patient_email parameters.	2021-11-05	not yet calculated	CVE-2021-39416 MISC MISC MISC
sitecore -- xp	Sitecore XP 7.5 Initial Release to Sitecore XP 8.2 Update-7 is vulnerable to an insecure deserialization attack where it is possible to achieve remote command execution on the machine. No authentication or special configuration is required to exploit this vulnerability.	2021-11-05	not yet calculated	CVE-2021-42237 MISC MISC MISC
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager 3.x through 3.35.0 allows attackers to access the SSL Certificates Loading function via a low-privileged account.	2021-11-02	not yet calculated	CVE-2021-42568 MISC MISC
sourcecodester -- engineers_online_portal	A file upload vulnerability exists in Sourcecodester Engineers Online Portal in PHP via dashboard_teacher.php, which allows changing the avatar through teacher_avatar.php. Once an avatar gets uploaded it is getting uploaded to the /admin/uploads/ directory, and is accessible by all users. By uploading a php webshell containing "<?php system($_GET["cmd"]); ?>" the attacker can execute commands on the web server with - /admin/uploads/php-webshell?cmd=id.	2021-11-05	not yet calculated	CVE-2021-42669 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sourcecodester -- engineers_online_portal	A Stored Cross Site Scripting (XSS) Vulneraibiilty exists in Sourcecodester Engineers Online Portal in PHP via the (1) Quiz title and (2) quiz description parameters to add_quiz.php. An attacker can leverage this vulnerability in order to run javascript commands on the web server surfers behalf, which can lead to cookie stealing and more.	2021-11-05	not yet calculated	CVE-2021-42664 MISC MISC MISC
sourcecodester -- engineers_online_portal	An SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the login form inside of index.php, which can allow an attacker to bypass authentication.	2021-11-05	not yet calculated	CVE-2021-42665 MISC MISC MISC
sourcecodester -- engineers_online_portal	A SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter to quiz_question.php, which could let a malicious user extract sensitive data from the web server and in some cases use this vulnerability in order to get a remote code execution on the remote web server.	2021-11-05	not yet calculated	CVE-2021-42666 MISC MISC MISC
sourcecodester -- engineers_online_portal	A SQL Injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter in the my_classmates.php web page.. As a result, an attacker can extract sensitive data from the web server and in some cases can use this vulnerability in order to get a remote code execution on the remote web server.	2021-11-05	not yet calculated	CVE-2021-42668 MISC MISC
sourcecodester -- engineers_online_portal	An incorrect access control vulnerability exists in Sourcecodester Engineers Online Portal in PHP in nia_munoz_monitoring_system/admin/uploads. An attacker can leverage this vulnerability in order to bypass access controls and access all the files uploaded to the web server without the need of authentication or authorization.	2021-11-05	not yet calculated	CVE-2021-42671 MISC MISC
sourcecodester -- engineers_online_portal	A SQL injection vulnerability exists in Sourcecodester Engineers Online Portal in PHP via the id parameter to the announcements_student.php web page. As a result a malicious user can extract sensitive data from the web server and in some cases use this vulnerability in order to get a remote code execution on the remote web server.	2021-11-05	not yet calculated	CVE-2021-42670 MISC MISC
sourcecodester -- online_event_booking_and_reservation_system	A SQL Injection vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP in event-management/views. An attacker can leverage this vulnerability in order to manipulate the sql query performed. As a result he can extract sensitive data from the web server and in some cases he can use this vulnerability in order to get a remote code execution on the remote web server.	2021-11-05	not yet calculated	CVE-2021-42667 MISC MISC
sourcecodester -- online_event_booking_and_reservation_system	An HTML injection vulnerability exists in Sourcecodester Online Event Booking and Reservation System in PHP/MySQL via the msg parameter to /event-management/index.php. An attacker can leverage this vulnerability in order to change the visibility of the website. Once the target user clicks on a given link he will display the content of the HTML code of the attacker's choice.	2021-11-05	not yet calculated	CVE-2021-42663 MISC MISC
stivasoft -- fundraising_script	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a SQL injection vulnerability via the pjActionLoadForm function.	2021-11-05	not yet calculated	CVE-2020-22225 MISC
stivasoft -- fundraising_script	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a SQL injection vulnerability via the pjActionSetAmount function.	2021-11-05	not yet calculated	CVE-2020-22226 MISC
stivasoft -- fundraising_script	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the pjActionPreview function.	2021-11-05	not yet calculated	CVE-2020-22224 MISC
stivasoft -- fundraising_script	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the pjActionLoadCss function.	2021-11-05	not yet calculated	CVE-2020-22222 MISC
stivasoft -- fundraising_script	Stivasoft (Phpjabbers) Fundraising Script v1.0 was discovered to contain a SQL injection vulnerability via the pjActionLoad function.	2021-11-05	not yet calculated	CVE-2020-22223 MISC
talend -- data_catalog	An issue was discovered in Talend Data Catalog before 7.3-20210930. After setting up SAML/OAuth, authentication is not correctly enforced on the native login page. Any valid user from the SAML/OAuth provider can be used as the username with an arbitrary password, and login will succeed.	2021-11-05	not yet calculated	CVE-2021-42837 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `FusedBatchNorm` kernels is vulnerable to a heap OOB access. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41223 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `tf.ragged.cross` has an undefined behavior due to binding a reference to `nullptr`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41214 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions if `tf.tile` is called with a large input argument then the TensorFlow process will crash due to a `CHECK`-failure caused by an overflow. The number of elements in the output tensor is too much for the `int64_t` type and the overflow is detected via a `CHECK` statement. This aborts the process. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41198 MISC CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions if `tf.image.resize` is called with a large input argument then the TensorFlow process will crash due to a `CHECK`-failure caused by an overflow. The number of elements in the output tensor is too much for the `int64_t` type and the overflow is detected via a `CHECK` statement. This aborts the process. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41199 CONFIRM MISC MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions if `tf.summary.create_file_writer` is called with non-scalar arguments code crashes due to a `CHECK`-fail. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41200 MISC CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions while calculating the size of the output within the `tf.range` kernel, there is a conditional statement of type `int64 = condition ? int64 : double`. Due to C++ implicit conversion rules, both branches of the condition will be cast to `double` and the result would be truncated before the assignment. This result in overflows. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41202 CONFIRM MISC MISC MISC MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions an attacker can trigger undefined behavior, integer overflows, segfaults and `CHECK`-fail crashes if they can change saved checkpoints from outside of TensorFlow. This is because the checkpoints loading infrastructure is missing validation for invalid file formats. The fixes will be included in TensorFlow 2.7.0. We will also cherrypick these commits on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41203 CONFIRM MISC MISC MISC MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions during TensorFlow's Grappler optimizer phase, constant folding might attempt to deep copy a resource tensor. This results in a segfault, as these tensors are supposed to not change. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41204 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions several TensorFlow operations are missing validation for the shapes of the tensor arguments involved in the call. Depending on the API, this can result in undefined behavior and segfault or `CHECK`-fail related crashes but in some scenarios writes and reads from heap populated arrays are also possible. We have discovered these issues internally via tooling while working on improving/testing GPU op determinism. As such, we don't have reproducers and there will be multiple fixes for these issues. These fixes will be included in TensorFlow 2.7.0. We will also cherrypick these commits on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41206 MISC MISC MISC MISC CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `ParallelConcat` misses some input validation and can produce a division by 0. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41207 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `tf.ragged.cross` can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41212 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the implementations for convolution operators trigger a division by 0 if passed empty filter tensor arguments. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41209 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for the `Cudnn*` operations in TensorFlow can be tricked into accessing invalid memory, via a heap buffer overflow. This occurs because the ranks of the `input`, `input_h` and `input_c` parameters are not validated, but code assumes they have certain values. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41221 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions TensorFlow's Grappler optimizer has a use of unitialized variable. If the `train_nodes` vector (obtained from the saved model that gets optimized) does not contain a `Dequeue` node, then `dequeue_node` is left unitialized. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41225 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SparseBinCount` is vulnerable to a heap OOB access. This is because of missing validation between the elements of the `values` argument and the shape of the sparse output. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41226 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the `ImmutableConst` operation in TensorFlow can be tricked into reading arbitrary memory contents. This is because the `tstring` TensorFlow string class has a special case for memory mapped strings but the operation itself does not offer any support for this datatype. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41227 CONFIRM MISC MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `AllToAll` can be made to execute a division by 0. This occurs whenever the `split_count` argument is 0. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41218 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions TensorFlow's `saved_model_cli` tool is vulnerable to a code injection as it calls `eval` on user supplied strings. This can be used by attackers to run arbitrary code on the plaform where the CLI tool runs. However, given that the tool is always run manually, the impact of this is not severe. We have patched this by adding a `safe` flag which defaults to `True` and an explicit warning for users. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41228 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SplitV` can trigger a segfault is an attacker supplies negative arguments. This occurs whenever `size_splits` contains more than one value and at least one value is negative. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41222 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `DeserializeSparse` can trigger a null pointer dereference. This is because the shape inference function assumes that the `serialize_sparse` tensor is a tensor with positive rank (and having `3` as the last dimension). The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41215 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the code for boosted trees in TensorFlow is still missing validation. As a result, attackers can trigger denial of service (via dereferencing `nullptr`s or via `CHECK`-failures) as well as abuse undefined behavior (binding references to `nullptr`s). An attacker can also read and write from heap buffers, depending on the API that gets used and the arguments that are passed to the call. Given that the boosted trees implementation in TensorFlow is unmaintained, it is recommend to no longer use these APIs. We will deprecate TensorFlow's boosted trees APIs in subsequent releases. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41208 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `tf.math.segment_*` operations results in a `CHECK`-fail related abort (and denial of service) if a segment id in `segment_ids` is large. This is similar to CVE-2021-29584 (and similar other reported vulnerabilities in TensorFlow, localized to specific APIs): the implementation (both on CPU and GPU) computes the output shape using `AddDim`. However, if the number of elements in the tensor overflows an `int64_t` value, `AddDim` results in a `CHECK` failure which provokes a `std::abort`. Instead, code should use `AddDimWithStatus`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41195 CONFIRM MISC MISC MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the Keras pooling layers can trigger a segfault if the size of the pool is 0 or if a dimension is negative. This is due to the TensorFlow's implementation of pooling operations where the values in the sliding window are not checked to be strictly positive. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41196 MISC CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions TensorFlow allows tensor to have a large number of dimensions and each dimension can be as large as desired. However, the total number of elements in a tensor must fit within an `int64_t`. If an overflow occurs, `MultiplyWithoutOverflow` would return a negative result. In the majority of TensorFlow codebase this then results in a `CHECK`-failure. Newer constructs exist which return a `Status` instead of crashing the binary. This is similar to CVE-2021-29584. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41197 CONFIRM MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affeced versions during execution, `EinsumHelper::ParseEquation()` is supposed to set the flags in `input_has_ellipsis` vector and `*output_has_ellipsis` boolean to indicate whether there is ellipsis in the corresponding inputs and output. However, the code only changes these flags to `true` and never assigns `false`. This results in unitialized variable access if callers assume that `EinsumHelper::ParseEquation()` always sets these flags. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41201 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the async implementation of `CollectiveReduceV2` suffers from a memory leak and a use after free. This occurs due to the asynchronous computation and the fact that objects that have been `std::move()`d from are still accessed. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, as this version is the only one that is also affected.	2021-11-05	not yet calculated	CVE-2021-41220 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the code for sparse matrix multiplication is vulnerable to undefined behavior via binding a reference to `nullptr`. This occurs whenever the dimensions of `a` or `b` are 0 or less. In the case on one of these is 0, an empty output tensor should be allocated (to conserve the invariant that output tensors are always allocated when the operation is successful) but nothing should be written to it (that is, we should return early from the kernel implementation). Otherwise, attempts to write to this empty tensor would result in heap OOB access. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41219 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference functions for the `QuantizeAndDequantizeV*` operations can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41205 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the process of building the control flow graph for a TensorFlow model is vulnerable to a null pointer exception when nodes that should be paired are not. This occurs because the code assumes that the first node in the pairing (e.g., an `Enter` node) always exists when encountering the second node (e.g., an `Exit` node). When this is not the case, `parent` is `nullptr` so dereferencing it causes a crash. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41217 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the implementation of `SparseFillEmptyRows` can be made to trigger a heap OOB access. This occurs whenever the size of `indices` does not match the size of `values`. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41224 MISC CONFIRM
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference functions for `SparseCountSparseOutput` can trigger a read outside of bounds of heap allocated array. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41210 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference code for `QuantizeV2` can trigger a read outside of bounds of heap allocated array. This occurs whenever `axis` is a negative value less than `-1`. In this case, we are accessing data before the start of a heap buffer. The code allows `axis` to be an optional argument (`s` would contain an `error::NOT_FOUND` error code). Otherwise, it assumes that `axis` is a valid index into the dimensions of the `input` tensor. If `axis` is less than `-1` then this results in a heap OOB read. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, as this version is the only one that is also affected.	2021-11-05	not yet calculated	CVE-2021-41211 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the shape inference function for `Transpose` is vulnerable to a heap buffer overflow. This occurs whenever `perm` contains negative elements. The shape inference function does not validate that the indices in `perm` are all valid. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41216 CONFIRM MISC
tensorflow -- tensorflow	TensorFlow is an open source platform for machine learning. In affected versions the code behind `tf.function` API can be made to deadlock when two `tf.function` decorated Python functions are mutually recursive. This occurs due to using a non-reentrant `Lock` Python object. Loading any model which contains mutually recursive functions is vulnerable. An attacker can cause denial of service by causing users to load such models and calling a recursive `tf.function`, although this is not a frequent scenario. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.	2021-11-05	not yet calculated	CVE-2021-41213 MISC CONFIRM
vim -- vim	vim is vulnerable to Stack-based Buffer Overflow	2021-11-05	not yet calculated	CVE-2021-3928 CONFIRM MISC
vim -- vim	vim is vulnerable to Heap-based Buffer Overflow	2021-11-05	not yet calculated	CVE-2021-3927 CONFIRM MISC
worx -- automation_suite	Improper Input Validation vulnerability in PC Worx Automation Suite of Phoenix Contact up to version 1.88 could allow an attacker with a manipulated project file to unpack arbitrary files outside of the selected project directory.	2021-11-04	not yet calculated	CVE-2021-34597 CONFIRM
wp -- dsgvo_tools	WP DSGVO Tools (GDPR) <= 3.1.23 had an AJAX action, ‘admin-dismiss-unsubscribe‘, which lacked a capability check and a nonce check and was available to unauthenticated users, and did not check the post type when deleting unsubscription requests. As such, it was possible for an attacker to permanently delete an arbitrary post or page on the site by sending an AJAX request with the “action” parameter set to “admin-dismiss-unsubscribe” and the “id” parameter set to the post to be deleted. Sending such a request would move the post to the trash, and repeating the request would permanently delete the post in question.	2021-11-05	not yet calculated	CVE-2021-42359 MISC

Back to top

This product is provided subject to this Notification and this Privacy & Use policy.

Having trouble viewing this message? View it as a webpage.

You are subscribed to updates from the Cybersecurity and Infrastructure Security Agency (CISA)
Manage Subscriptions | Privacy Policy | Help

Connect with CISA:
Facebook | Twitter | Instagram | LinkedIn | YouTube

Powered by
GOVDELIVERY

Privacy Policy | Cookie Statement | Help